0350914

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１２月２７日

出願番号
Application Number: 特願２００２－３８１３８０

[ST. 10/C]: [ＪＰ２００２－３８１３８０]

出願人
Applicant(s): 株式会社東芝

２００３年 ７月 ８日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号 出証特２００３－３０５４００８

【書類名】　特許願
【整理番号】　A000204959
【提出日】　平成14年12月27日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F 15/00
【発明の名称】　電子透かし埋込装置、電子透かし検出装置、電子透かし埋込方法、電子透かし検出方法及びプログラム
【請求項の数】　24
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
【氏名】　村谷　博文
【特許出願人】
【識別番号】　000003078
【氏名又は名称】　株式会社　東芝
【代理人】
【識別番号】　100058479
【弁理士】
【氏名又は名称】　鈴江　武彦
【電話番号】　03-3502-3181
【選任した代理人】
【識別番号】　100084618
【弁理士】
【氏名又は名称】　村松　貞男
【選任した代理人】
【識別番号】　100068814
【弁理士】
【氏名又は名称】　坪井　淳

【選任した代理人】
　【識別番号】　100092196
　【弁理士】
　【氏名又は名称】　橋本　良郎
【選任した代理人】
　【識別番号】　100091351
　【弁理士】
　【氏名又は名称】　河野　哲
【選任した代理人】
　【識別番号】　100088683
　【弁理士】
　【氏名又は名称】　中村　誠
【選任した代理人】
　【識別番号】　100070437
　【弁理士】
　【氏名又は名称】　河井　将次
【手数料の表示】
　【予納台帳番号】　011567
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子透かし埋込装置、電子透かし検出装置、電子透かし埋込方法、電子透かし検出方法及びプログラム

【特許請求の範囲】

【請求項１】　透かし情報として入力された位相不変量に対応する第１の関数を生成する関数生成手段と、

入力された鍵情報に基づいて掻き混ぜ関数を生成し、該掻き混ぜ関数と前記第１の関数とを合成した第２の関数を計算する関数掻き混ぜ手段と、

入力された埋込対象コンテンツに対して前記第２の関数を埋め込む関数埋め込み手段とを備えたことを特徴とする電子透かし埋込装置。

【請求項２】　前記第１の関数は、前記埋込対象コンテンツにおける埋め込む位置に関する基底空間から埋め込む量に関する対象空間への前記位相不変量に基づく写像を与える関数であることを特徴とする請求項１に記載の電子透かし埋込装置。

【請求項３】　前記埋込対象コンテンツは、静止画像又は動画像データであり、

前記埋め込む位置に関する基底空間は、静止画像又は動画像データにおける画素位置のなす空間であり、

前記埋め込む量に関する対象空間は、静止画像又は動画像データにおける画素値に関する所定のベクトルのなす空間であることを特徴とする請求項１または２に記載の電子透かし埋込装置。

【請求項４】　前記埋込対象コンテンツは、音声データであり、

前記埋め込む位置に関する基底空間は、音声データにおける時間的サンプリング位置のなす空間であり、

前記埋め込む量に関する対象空間は、音声データにおける振幅値に関する所定のベクトルのなす空間であることを特徴とする請求項１または２に記載の電子透かし埋込装置。

【請求項５】　前記関数生成手段は、前記第１の関数を表現する第１の関数値を生成することを特徴とする請求項１ないし４のいずれか１項に記載の電子透

かし埋込装置。

【請求項６】　前記関数掻き混ぜ手段は、前記関数生成手段により生成された前記第１の関数値に対して前記掻き混ぜ関数を適用して、前記第２の関数を表現する第２の関数値を生成することを特徴とする請求項５に記載の電子透かし埋込装置。

【請求項７】　前記第１及び第２の関数値は、前記埋込対象コンテンツにおける各埋め込む位置に対する各埋め込む量を示すものであることを特徴とする請求項５または６に記載の電子透かし埋込装置。

【請求項８】　前記関数掻き混ぜ手段は、前記鍵情報に基づくブロック暗号によって、前記第１の関数値を掻き混ぜて、前記第２の関数値を生成することを特徴とする請求項６または７に記載の電子透かし埋込装置。

【請求項９】　前記関数埋め込み手段は、前記第２の関数値に基づいて前記埋込対象コンテンツの内容を変更することによって、前記位相不変量を埋め込むことを特徴とする請求項６ないし８のいずれか１項に記載の電子透かし埋込装置。

【請求項１０】　前記位相不変量は、ホモトピー不変量であることを特徴とする請求項１ないし９のいずれか１項に記載の電子透かし埋込装置。

【請求項１１】　入力された検出対象コンテンツに埋め込まれている第３の関数を検出する関数検出手段と、

入力された鍵情報に基づいて掻き混ぜ戻し関数を生成し、該掻き混ぜ戻し関数と前記第３の関数を合成した第４の関数を計算する関数掻き混ぜ戻し手段と、

前記第４の関数に基づいて透かし情報としての位相不変量を計算する位相不変量計算手段とを備えたことを特徴とする電子透かし検出装置。

【請求項１２】　前記第４の関数は、前記埋込対象コンテンツにおける埋め込む位置に関する基底空間から埋め込む量に関する対象空間への前記位相不変量に基づく写像を与える関数であることを特徴とする請求項１１に記載の電子透かし検出装置。

【請求項１３】　前記埋込対象コンテンツは、静止画像又は動画像データであり、

前記埋め込む位置に関する基底空間は、静止画像又は動画像データにおける画素位置のなす空間であり、

前記埋め込む量に関する対象空間は、静止画像又は動画像データにおける画素値に関する所定のベクトルのなす空間であることを特徴とする請求項１１または１２に記載の電子透かし検出装置。

【請求項１４】　前記埋込対象コンテンツは、音声データであり、

前記埋め込む位置に関する基底空間は、音声データにおける時間的サンプリング位置のなす空間であり、

前記埋め込む量に関する対象空間は、音声データにおける振幅値に関する所定のベクトルのなす空間であることを特徴とする請求項１１または１２に記載の電子透かし検出装置。

【請求項１５】　前記関数検出手段は、前記第３の関数を表現する第３の関数値を検出することを特徴とする請求項１１ないし１４のいずれか１項に記載の電子透かし検出装置。

【請求項１６】　前記関数掻き混ぜ戻し手段は、前記関数検出手段により検出された前記第３の関数値に対して前記掻き混ぜ戻し関数を適用して、前記第４の関数を表現する第４の関数値を生成することを特徴とする請求項１５に記載の電子透かし検出装置。

【請求項１７】　前記第３及び第４の関数値は、前記埋込対象コンテンツにおける各埋め込む位置に対する各埋め込む量を示すものであることを特徴とする請求項１５または１６に記載の電子透かし検出装置。

【請求項１８】　前記関数掻き混ぜ戻し手段は、前記鍵情報に基づくブロック暗号によって、前記第３の関数値を掻き混ぜ戻して、前記第４の関数値を生成することを特徴とする請求項１６または１７に記載の電子透かし検出装置。

【請求項１９】　前記第４の関数は、前記埋込対象コンテンツにおける埋め込む位置に関する基底空間から埋め込む量に関する対象空間への前記位相不変量に基づく写像を与える関数であって、該写像を決定付けるパラメータとして前記位相不変量によるパラメータを持つものであり、

前記位相不変量計算手段は、前記第４の関数値に基づいて前記写像を決定付け

るパラメータを求めることによって、前記位相不変量を計算することを特徴とする請求項１６ないし１８のいずれか１項に記載の電子透かし検出装置。

【請求項２０】　前記位相不変量は、ホモトピー不変量であることを特徴とする請求項１１ないし１９のいずれか１項に記載の電子透かし検出装置。

【請求項２１】　透かし情報として入力された位相不変量に対応する第１の関数を生成する関数生成ステップと、

入力された鍵情報に基づいて掻き混ぜ関数を生成し、該掻き混ぜ関数と前記第１の関数とを合成した第２の関数を計算する関数掻き混ぜステップと、

入力された埋込対象コンテンツに対して前記第２の関数を埋め込む関数埋め込みステップとを有することを特徴とする電子透かし埋込方法。

【請求項２２】　入力された検出対象コンテンツに埋め込まれている第３の関数を検出する関数検出ステップと、

入力された鍵情報に基づいて掻き混ぜ戻し関数を生成し、該掻き混ぜ戻し関数と前記第３の関数を合成した第４の関数を計算する関数掻き混ぜ戻しステップと、

前記第４の関数に基づいて透かし情報としての位相不変量を計算する位相不変量計算ステップとを有することを特徴とする電子透かし検出方法。

【請求項２３】　コンピュータを電子透かし埋込装置として機能させるためのプログラムであって、

透かし情報として入力された位相不変量に対応する第１の関数を生成する関数生成機能と、

入力された鍵情報に基づいて掻き混ぜ関数を生成し、該掻き混ぜ関数と前記第１の関数とを合成した第２の関数を計算する関数掻き混ぜ機能と、

入力された埋込対象コンテンツに対して前記第２の関数を埋め込む関数埋め込み機能とをコンピュータに実現させるためのプログラム。

【請求項２４】　コンピュータを電子透かし検出装置として機能させるためのプログラムであって、

入力された検出対象コンテンツに埋め込まれている第３の関数を検出する関数検出機能と、

入力された鍵情報に基づいて掻き混ぜ戻し関数を生成し、該掻き混ぜ戻し関数と前記第３の関数を合成した第４の関数を計算する関数掻き混ぜ戻し機能と、

前記第４の関数に基づいて透かし情報としての位相不変量を計算する位相不変量計算機能とをコンピュータに実現させるためのプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、デジタル・データ化された静止画データ、動画データ、音声データ、音楽データ等のコンテンツに対して透かし情報を埋め込む電子透かし埋込装置及び電子透かし埋込方法、コンテンツから透かし情報を検出する電子透かし検出装置及び電子透かし検出方法、並びにプログラムに関する。

【０００２】

【従来の技術】

（電子透かし）

電子透かし（ｄｉｇｉｔａｌ　ｗａｔｅｒｍａｒｋｉｎｇ）は、デジタルデータ化された静止画、動画、音声、音楽等のデジタル・コンテンツ（あるいは、デジタル著作物データ）に対して、品質劣化が目立たない程度の小さな変更を加えることで別の情報を埋め込む技術である。例えば、コンテンツの著作権者の識別情報、コンテンツの利用者の識別情報、コンテンツの著作権者の権利情報、コンテンツの利用条件、コンテンツの利用時に必要な秘密情報、コピー制御情報などの情報(以下、透かし情報と呼ぶ)を知覚が容易ではない状態となるように埋め込み、後に必要に応じて透かし情報をコンテンツから検出することによって利用制御、コピー制御を含む著作権保護を行ったり、二次利用の促進を行うものである。また、例えば、著作者の識別、所有権の証明、フィンガープリンティング、コンテンツの証明、放送の監視などの応用が提案されている。

【０００３】

（電子透かしの要件）

デジタル・コンテンツの不正利用の防止を目的とする場合、透かし情報は、そのコンテンツに対して通常に施されると想定される各種の操作や意図的な攻撃に

よって、消失したり改ざんされたりしないような性質（ｒｏｂｕｓｔｎｅｓｓ：ロバスト性）を持つ必要がある。

【０００４】

（幾何学的改変）

デジタル・コンテンツが画像（静止画や動画）の場合、幾何学的変形によって、電子透かしを消失させる攻撃がある。幾何学的変形とは、画像の座標変換である。幾何学的変形は、画素の位置を変えてしまうため、電子透かしの方式によっては、検出時に、画素の位置の同期がとれずに、正しく透かし情報が読み取れないという問題が生ずる。

【０００５】

幾何学的変形は、２つに大別される。大域的変形と局所的変形である。大域的変形は、画像全体のスケーリング、回転、平行移動であり、アフィン変換として表現される。一方、局所的変換は、大域的変換のように位置によらないパラメータによって表現される変形だけでなく、局所的なパラメータによって表現される変換を含む変換である。大域的変換は、局所的変換の特殊な場合である。

【０００６】

（位相的電子透かし方式）

同相な空間には、位相不変量と呼ばれる不変な性質が存在し得ることが知られている。例えば、ホモトピー類がその例である（例えば、非特許文献１参照）。

【０００７】

そこで、局所的な幾何学的変形を同相写像とみなすことで、電子透かしを位相不変量と関連付けることが考えられる。この局所的な幾何学的変形に対するロバスト性を実現するための技術として、位相的電子透かし方式がある（例えば、特許文献１参照）。位相的電子透かし方式は、局所的な幾何学的変形の下で不変な位相不変量（例えば、ホモトピー類）を電子透かしとして埋め込む。電子透かしは、所定のホモトピー類ｂに属する関数Ψ_bによって表現されて埋め込まれる。電子透かしの検出は、検出された関数Ψ_b'からそのホモトピー類ｂを計算することで行われる。

【０００８】

【特許文献１】

特開２００２－１４２０９４

【０００９】

【非特許文献１】

岩波数学辞典第３版，位相空間，２２－３４，ホモトピー理論，１１４２－１１５０

【００１０】

【発明が解決しようとする課題】

従来の電子透かし技術では、電子透かしを位相不変量としてコンテンツに埋め込むにあたって、素直な埋め込み方をしていた。

【００１１】

本発明は、上記事情を考慮してなされたもので、ＳｔｉｒＭａｒｋ攻撃やＤ－Ａ－Ｄ－変換などの局所的変形に対する耐性を持つとともに、電子透かしのアルゴリズムの全部又は一部が開示されたとしてもなお安全であるような電子透かし埋込装置及び電子透かし検出装置、電子透かし埋込方法及び電子透かし検出方法、並びにプログラムを提供することを目的とする。

【００１２】

【課題を解決するための手段】

本発明に係る電子透かし埋込装置は、透かし情報として入力された位相不変量に対応する第１の関数を生成する関数生成手段と、入力された鍵情報に基づいて掻き混ぜ関数を生成し、該掻き混ぜ関数と前記第１の関数とを合成した第２の関数を計算する関数掻き混ぜ手段と、入力された埋込対象コンテンツに対して前記第２の関数を埋め込む関数埋め込み手段とを備えたことを特徴とする。

【００１３】

また、本発明に係る電子透かし検出装置は、入力された検出対象コンテンツに埋め込まれている第３の関数を検出する関数検出手段と、入力された鍵情報に基づいて掻き混ぜ戻し関数を生成し、該掻き混ぜ戻し関数と前記第３の関数を合成した第４の関数を計算する関数掻き混ぜ戻し手段と、前記第４の関数に基づいて透かし情報としての位相不変量を計算する位相不変量計算手段とを備えたことを

特徴とする。

【００１４】

好ましくは、前記第１、第４の関数は、前記埋込対象コンテンツにおける埋め込む位置に関する基底空間から埋め込む量に関する対象空間への前記位相不変量に基づく写像を与える関数であるようにしてもよい。

【００１５】

好ましくは、前記第１～第４の関数値は、前記埋込対象コンテンツにおける各埋め込む位置に対する各埋め込む量を示すものであるようにしてもよい。

【００１６】

好ましくは、前記関数掻き混ぜ手段は、前記鍵情報に基づくブロック暗号によって、前記第１の関数値を掻き混ぜて、前記第２の関数値を生成するようにしてもよい。

【００１７】

好ましくは、前記関数掻き混ぜ戻し手段は、前記関数検出手段により検出された前記第３の関数値に対して前記掻き混ぜ戻し関数を適用して、前記第４の関数を表現する第４の関数値を生成するようにしてもよい。

【００１８】

なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムとしても成立し、該プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【００１９】

本発明では、対象となるデジタル・コンテンツ（例えば、画像データ）に透かし情報を埋め込む際、対象コンテンツに埋め込むべき透かし情報に対応する所定の位相不変量（例えば、ホモトピー不変量）を得て、対象コンテンツの内容のうち予め定められた部分を変更することによって、該コンテンツに該位相不変量を

設定する。

また、本発明では、対象となるデジタル・コンテンツから該コンテンツに埋め込まれた透かし情報を検出する際、対象コンテンツの内容のうち予め定められた部分に基づいて、該コンテンツに設定された所定の位相不変量を検出し、検出された該所定の位相不変量に対応する透かし情報を出力する。

例えば、透かし情報としてコピー可を指示する制御情報を埋め込む際に、例えばホモトピー類の全体が整数全体Ｚと同型である場合に、ホモトピー類＝＋１（もちろん、＋１以外の値でもよい）となるように画素値を変更し、コピー不可とする場合に、ホモトピー類＝－１（もちろん、－１以外の値でもよい）となるように画素値を変更する。また、例えば、透かし情報として著作権者等の識別番号を埋め込む場合に、識別番号１が指定されたならば、ホモトピー類＝１（もちろん、１以外の値でもよい）となるように画素値を変更し、識別番号２が指定されたならば、ホモトピー類＝２（もちろん、２以外の値でもよい）となるように画素値を変更する。

【００２０】

本発明によれば、埋め込むべき透かし情報に対応する位相不変量を対象コンテンツに設定するようにしたので、たとえ流通経路などでＳｔｉｒＭａｒｋ攻撃やＤ－Ａ－Ｄ－変換などの局所的変形を受けてもコンテンツに設定した位相不変量は維持・保存される。そして、局所的変形を受けたか否かにかかわたずコンテンツから正しい位相不変量を検出し、対応する正しい透かし情報を得ることができる。

【００２１】

また、コンテンツのビット列の変化が小さくなるように位相不変量を表現するデータを書き込むことによって、なるべくコンテンツに影響を与えないようにすることができる。

【００２２】

これに加えて、本発明では、埋め込み時には、第１の関数（値）を埋め込むのではなく、第１の関数（値）に対して鍵情報に基づく掻き混ぜを行った後に、これによって得られた第２の関数（値）を埋め込むので、検出時には、第３の関数

（値）から位相不変量を求めることはできず、埋め込み時に用いた鍵情報に対応する鍵情報があってはじめて、該鍵情報に基づく掻き混ぜ戻しを行った後に、これによって得られた第４の関数（値）（鍵情報が正しければ、第４の関数（値）＝第１の関数（値）となる）をもとにして、正しい位相不変量を得ることができる。第３の関数（値）からは、電子透かしの存在自体を知ることも難しく、それを知っていたとしても、正しい位相不変量を得ることはできず、また、正しい鍵情報がなければ、第４の関数（値）からも正しい位相不変量を求めることはできない。

【００２３】

なお、本発明では、鍵情報に基づく掻き混ぜ及び掻き混ぜ戻しは、従来の単なるスクランブル及びデスクランブルではない。従来のように単純に画像をスクランブルした後に、幾何学的改変を受けると、デスクランブルして元に戻せなくなることがあるが、本発明によれば、鍵情報に基づく掻き混ぜを行った後に、幾何学的改変を受けても、鍵情報に基づく掻き混ぜ戻しができるようになっている。

【００２４】

このように、本発明によれば、ＳｔｉｒＭａｒｋ攻撃やＤ－Ａ－Ｄ－変換などの局所的変形に対する耐性を持つとともに、電子透かしのアルゴリズムの全部又は一部が開示されたとしてもなお安全であるような電子透かしを実現することができる。

【００２５】

【発明の実施の形態】

以下、図面を参照しながら発明の実施の形態を説明する。

【００２６】

本発明は、コンテンツ（例えば、デジタルデータ化された静止画、動画、音声、音楽等）に対して様々な透かし情報（例えば、コンテンツの著作権者や利用者の識別情報、著作権者の権利情報、コンテンツの利用条件、その利用時に必要な秘密情報、コピー制御情報等、あるいはそれらを組み合わせたものなど）を様々な目的（例えば、利用制御、コピー制御を含む著作権保護、二次利用の促進等）で埋め込み、検出する場合に適用可能である。

【００２７】

図１に、本発明の一実施形態に係る電子透かし埋込装置と電子透かし検出装置が適用されるシステムの概念図を示す。

【００２８】

電子透かし埋込装置１は、埋め込み対象となるコンテンツに透かし情報を埋め込むもので、対象コンテンツとこれに埋め込むべき透かし情報と鍵情報が入力され、電子透かし情報埋め込み済みコンテンツを出力する。電子透かし埋込装置１は、コンテンツ提供側に備えられ、管理される。

【００２９】

電子透かし埋込装置１により得られた電子透かし情報埋め込み済みコンテンツは、記憶媒体や通信媒体などを媒介とした流通経路３を経て流通する。その際、流通経路３では、コンテンツに対してＳｔｉｒＭａｒｋ攻撃やＤ－Ａ－Ｄ－変換などの局所的変換がなされることがある（局所的変換は、ユーザの故意によってなされることもあるし、ユーザの故意あるいは認識なくしてなされることもある）。

【００３０】

電子透かし検出装置２は、検出対象となるコンテンツから透かし情報を検出するもので、対象コンテンツと鍵情報が入力され、検出された透かし情報を出力する。電子透かし検出装置２は、コンテンツ利用時の著作権保護を目的としてユーザ側のコンテンツ利用装置に内蔵される場合や、コンテンツ提供側が流通を経たコンテンツから電子透かしを検出することを目的としてコンテンツ提供側に備えられる場合がある。

【００３１】

本実施形態では、詳しくは後述するように、電子透かし埋込装置１は、ＳｔｉｒＭａｒｋ攻撃やＤ－Ａ－Ｄ－変換などがなされても透かし情報の内容が維持・保存されるように透かし情報を埋め込むので、流通経路３においてコンテンツに対してＳｔｉｒＭａｒｋ攻撃やＤ－Ａ－Ｄ－変換などがなされても、電子透かし検出装置２は、電子透かし埋込装置１で埋め込まれた透かし情報を正しく検出することができる。

【００３２】

また、電子透かし検出装置２は、電子透かし埋込装置１で当該コンテンツについて使用した鍵情報に対応する正当な鍵情報（例えば、共通鍵暗号方式が用いられる場合には、電子透かし埋込装置１で使用した鍵情報と同一の鍵情報）を用いることによってのみ、当該コンテンツに埋め込まれた透かし情報を正しく検出することができるので、電子透かしのアルゴリズムが開示されたとしても鍵情報が開示されていなければ安全であるように構成することができるものとなっている。

【００３３】

なお、本実施形態では、電子透かし埋込装置１にはデジタル・コンテンツが入力され、電子透かし検出装置２からはデジタル・コンテンツが出力されるものとして説明するが、電子透かし埋込装置１に、入力されたアナログ・コンテンツを透かし情報の埋め込みに先立ってデジタル・コンテンツに変換する機能を搭載してもよいし、およびまたは、電子透かし検出装置２に、入力されたアナログ・コンテンツを透かし情報の検出に先立ってデジタル・コンテンツに変換する機能を搭載してもよい。

【００３４】

電子透かし埋込装置１は、ソフトウェア（プログラム）としてもハードウェアとしても実現可能である。同様に、電子透かし検出装置２は、ソフトウェア（プログラム）としてもハードウェアとしても実現可能である。

電子透かし埋込装置１および電子透かし検出装置２をコンテンツ提供側で用いる場合には、それらを一体化して実現することも可能である。

電子透かし検出装置２をユーザ側のコンテンツ利用装置に内蔵する場合には、ユーザにより電子透かし検出装置２に対する操作や解析あるいは攻撃などができないように安全に作り込んでおくのが望ましい。

【００３５】

なお、以下で示す構成図は、装置の機能ブロック図としても成立し、また、ソフトウェア（プログラム）の機能モジュール図あるいは手順図としても成立するものである。

【００３６】

本実施形態では、デジタル・コンテンツの一例として主に動画像データを対象とした場合を例にとって説明するが、静止画像データや音声データ等の他のメディアのデータを対象とすることも可能である。なお、ＳｔｉｒＭａｒｋ攻撃やＤ－Ａ－Ｄ－変換などの局所的変形は、例えば、動画像については、フレーム単位で処理する場合には、データの幾何学的変形であり、複数フレームにわたって時間的位置を考慮して処理する場合にはデータの幾何学的変形および時間軸方向の変形（時空間的変形）である。また、静止画の場合には、静止画データの幾何学的変形であり、音声の場合には、音声データの時間軸方向の変形である。

【００３７】

さて、本実施形態は、透かし情報を位相不変量（ｔｏｐｏｌｏｇｉｃａｌ　ｉｎｖａｒｉａｎｔ）としてコンテンツに埋め込む（例えば対象コンテンツから得られる位相不変量が透かし情報に対応する値になるように対象コンテンツの画素値等を操作する）ことによって、ＳｔｉｒＭａｒｋ攻撃やＤ－Ａ－Ｄ－変換などの局所的変形に対して耐性を持つようにしたものであるが、以下では、電子透かしとして位相不変量を直接用いる場合を例にとって説明するものとし、また、位相不変量の一例としてホモトピー不変量（ｈｏｍｏｔｏｐｙ　ｉｎｖａｒｉａｎｔ）を用いた構成例について説明する。

【００３８】

なお、電子透かしとして位相不変量を直接用いる代わりに、電子透かし埋込装置１側に、与えられた透かし情報を埋め込むべき位相不変量に変換する透かし情報・位相不変量変換部を設け、電子透かし検出装置２側に、検出された位相不変量を対応する透かし情報に変換する位相不変量・透かし情報変換部を設けるようにしてもよい。

【００３９】

また、位相不変量やホモトピー不変量やホモトピー類などの電子透かしへの応用については、特許文献１に開示されたものと同様の考え方を用いることができる。

【００４０】

図２に、本発明の一実施形態に係る電子透かし埋込装置の構成例を示す。

【００４１】

本電子透かし埋込装置は、埋め込み対象のデジタルコンテンツ（本例では、動画像）と、埋め込むべき電子透かしであるホモトピー類と、鍵情報とを入力として、電子透かしの埋め込み済みコンテンツを出力する。

【００４２】

図２に示されるように、本電子透かし埋込装置は、関数生成部１１、関数掻き混ぜ部１２、関数埋め込み部１３を備えている。

【００４３】

図３に、本実施形態の電子透かし埋込装置の処理手順の一例を示す。

電子透かしを埋め込む対象となる埋め込み対象画像、鍵情報、透かし情報（本例では、ホモトピー類）を入力する（ステップＳ１）。

与えられたホモトピー類に属する関数を生成する（ステップＳ２）。

与えられた鍵情報に従い、掻き混ぜ関数を生成し、上記のホモトピー類に属する関数との合成関数を生成する（ステップＳ３）。

生成された合成関数を埋め込み対象画像に埋め込む（ステップＳ４）。

電子透かしを埋め込まれた埋め込み済み画像を出力する（ステップＳ５）。

【００４４】

まず、関数生成部１１の機能について説明する。

【００４５】

ここで、画像は、画素の集まりである。

【００４６】

画素は、画像中の位置と、その位置における色によって、記述される。

【００４７】

画像中の位置のなす空間Ｂを基底空間、色の空間Ｃを色空間と呼ぶ。例えば、静止画あるいは動画の１フレームの場合には、基底空間Ｂは、２次元の有限領域である。カラー画像の場合には、色空間Ｃは、３次元の有限領域である。

【００４８】

ｎ個（ｎ≧１とする）の色空間Ｃの積空間$C^n = C \times C \times \cdots \times C$の中に所定の

部分空間Ｔ⊂Ｃⁿを構成し、それを対象空間と呼ぶことにする。色空間Ｃの中に対象空間Ｔを包含する所定の部分空間Ｓ⊃Ｔを設定してあるものとし、これを掻き混ぜ空間と呼ぶ。

【００４９】

本例では、基底空間Ｂの同相写像に対する不変量を透かし情報とみなす。具体的には、位相不変量として、基底空間Ｂから対象空間Ｔへの写像が属するホモトピー類を利用する。

【００５０】

関数生成部１１は、埋め込むべき情報であるところのホモトピー類ｂが入力されたとき、それに属する関数Ψ_b：Ｂ→Ｔを生成する。

【００５１】

次に、関数掻き混ぜ部１２の機能について説明する。

【００５２】

関数掻き混ぜ部１２は、掻き混ぜ空間Ｓから掻き混ぜ空間Ｓへの写像であって、入力される鍵情報ｋに応じて異なる関数（掻き混ぜ関数）g_k：Ｓ→Ｓを生成し、この鍵情報ｋに基づく掻き混ぜ関数g_kと、関数生成部１１が生成したホモトピー類ｂに属する関数Ψ_bとの合成関数$g_k \circ \Psi_b$：Ｂ→Ｓを生成する（なお、○は、その前後に記述された関数の合成関数を表すものとする）。

【００５３】

次に、関数埋め込み部１３の機能について説明する。

【００５４】

関数埋め込み部１３は、関数掻き混ぜ部１２が生成した合成関数$g_k \circ \Psi_b$を、埋め込み対象画像に埋め込む。埋め込みは、基底空間Ｂの各点に対して、掻き混ぜ空間Ｓ中の値が、合成関数の与える値となるように、画像を変更することによって、実施する。そして、電子透かしを埋め込んだ対象画像を埋め込み済み画像として出力する。

【００５５】

図４に、本発明の一実施形態に係る電子透かし検出装置の構成例を示す。

【００５６】

本電子透かし検出装置は、検出対象のコンテンツ（本例では、動画像）と、鍵情報とを入力として、電子透かし情報であるホモトピー類を出力する。

【００５７】

図４に示されるように、本電子透かし検出装置は、関数検出部２１、関数掻き混ぜ戻し部２２、ホモトピー類計算部２３を備えている。

【００５８】

図５に、電子透かし検出装置の処理手順の一例を示す。

電子透かしを検出する対象となる検出対象画像、鍵情報を入力する（ステップＳ１１）。

検出対象画像から、埋め込まれている関数を読み取る（ステップＳ１２）。

【００５９】

与えられた鍵情報に従い、（前記の掻き混ぜ関数に対応する）掻き混ぜ戻し関数を生成し、上記の埋め込まれている関数との合成関数を生成する（ステップＳ１３）。

生成された合成関数の属するホモトピー類を計算する（ステップＳ１４）。

求められたホモトピー類を電子透かしとして出力する（ステップＳ１５）。

【００６０】

まず、関数検出部２１の機能について説明する。

【００６１】

関数検出部２１は、検出対象画像が与えられたとき、その画像から、基底空間Ｂの各点に対する掻き混ぜ空間Ｓにおける値を求めることによって、埋め込まれている関数Φ：Ｂ→Ｓを求める。

【００６２】

次に、関数掻き混ぜ戻し部２２の機能について説明する。

【００６３】

関数掻き混ぜ戻し部２２は、関数掻き混ぜ部１２と同様に、掻き混ぜ空間Ｓから掻き混ぜ空間Ｓへの写像であって、入力される鍵情報ｋに応じて異なる関数g_k^{-1}：Ｓ→Ｓを生成する。このg_k^{-1}は、先のg_kの逆となっている。すなわち、gk-1○gk＝１である。

【００６４】

関数掻き混ぜ戻し部２２は、さらに、この鍵情報ｋに基づく掻き混ぜ戻し関数g_k^{-1}と、関数生成部１１が生成した埋め込まれている関数Φとの合成関数$g_k^{-1}\bigcirc\Phi$：Ｂ→Ｓを生成する。

【００６５】

検出対象が、電子透かしを埋め込まれた画像であって、関数掻き混ぜ戻し部２２が、電子透かし埋込装置１の関数掻き混ぜ部１２が用いた鍵情報と同じ鍵情報ｋを用いるときは、関数掻き混ぜ戻し部２２により生成された合成関数Ξ：Ｂ→Ｓは、$\Xi=g_k^{-1}\bigcirc\Phi=g_k^{-1}\bigcirc g_k\bigcirc\Psi_b=\Psi_b$となる。この$\Psi_b$は、電子透かし埋込装置１の関数生成部１１が生成した、電子透かしとして与えられたホモトピー類ｂに属する関数（Ψ_b：Ｂ→Ｔ）である。従って、この合成関数Ξの値域は、対象空間Ｔ上にあることが期待される。つまり、Ξ：Ｓ→Ｔである。

【００６６】

関数掻き混ぜ戻し部２２が、当該検出対象画像について電子透かし埋込装置１の関数掻き混ぜ部１２が用いた鍵情報とは異なる鍵情報ｋ´を用いるときは、$\Xi'=g_{k'}^{-1}\bigcirc\Phi=g_{k'}^{-1}\bigcirc g_k\bigcirc\Psi_b$となって、一般的には、$\Xi'\neq\Psi_b$となり、合成関数Ξ´の値域は、Ｔ上に収まる保障がないの。よって、対象となったコンテンツが、電子透かしが埋め込まれた画像であるか否かを知ることは難しいし、正しいΞを知ることも（従って、埋め込まれている電子透かしの正しい内容を知ることも）難しい。

【００６７】

次に、ホモトピー類計算部２３の機能について説明する。

【００６８】

ホモトピー類計算部２３の機能は、関数掻き混ぜ戻し部２２により得られた合成関数Ξ：Ｂ→Ｔから、その合成関数の属するホモトピー類を計算する。そして、その結果を、得られた電子透かしとして出力する。

【００６９】

なお、ここでは、同一のコンテンツについて、電子透かし埋込装置１で用いる掻き混ぜ関数を決定付ける鍵情報と電子透かし検出装置２で用いる掻き混ぜ戻し

関数を決定付ける鍵情報とを同一のものとする場合を例とって説明しているが、電子透かし埋込装置１で生成する掻き混ぜ関数と、電子透かし検出装置２で生成する掻き混ぜ戻し関数とが、逆になるようにできさえすれば、電子透かし埋込装置１で用いる鍵情報と、電子透かし検出装置２で用いる鍵情報とが同一でないような構成にしてもよい。

【００７０】

以下、具体例を用いて本実施形態について説明する。

【００７１】

画像中の画素の位置のなす空間である基底空間Ｂは、本来は、例えば、縦５１２画素、横５１２画素からなるような、２次元有限領域であるが、この基底空間Ｂの周囲を１点と同一視するように変形することで、基底空間Ｂを２次元球面S^2であるとみなすことができる。この様子を、図６に示す。

【００７２】

この同一視により、基底空間Ｂの座標を、２次元球面の極座標（θ，ϕ）で表すことができる。ここで、$\theta \in [0, \pi)$、$\phi \in [0, 2\pi)$である。もとの基底空間Ｂの座標は（ｘ，ｙ）とし、$x \in [0, W)$、$y \in [0, H)$とする。ここで、ＷとＨは、画像の幅と高さである。このとき、（θ，ϕ）と（ｘ，ｙ）とは簡単な座標変換によって相互に変換できる。この座標変換は、例えば、次式で与えられる。

【００７３】

$$\theta = 2 \arctan\left[2/\left|\tan^2\left\{\pi/2(x/W-1/2)\right\}+\tan^2\left\{\pi/2(y/H-1/2)\right\}\right|\right]$$

$$\cos\Phi = \tan^2\left\{\pi/2(x/W-1/2)\right\}/\left|\tan^2\left\{\pi/2(x/W-1/2)\right\}+\tan^2\left\{\pi/2(y/H-1/2)\right\}\right|$$

$$\sin\Phi = \tan^2\left\{\pi/2(y/H-1/2)\right\}/\left|\tan^2\left\{\pi/2(x/W-1/2)\right\}+\tan^2\left\{\pi/2(y/H-1/2)\right\}\right|$$

次に、画素の色としては濃淡を例にとる（画像として濃淡画像を例にとる）。従って、色空間Ｃは、輝度値だけの１次元領域Ｃ＝［０，２５６）であるとする。

【００７４】

ここでは、一例として、６ｇ枚（ｇは予め定められた整数）のフレームから得られる積空間C^{6g}を考える。連続する６ｇ枚のフレームについて、連続するｇ枚のフレームごとに分割して、６つのグループを作る。最初のグループ（G_0）と次のグループ（G_1）において、基底空間Ｂの各点ごとに、グループG_0の輝度値の和から、グループG_1の輝度値の和を引く。これによって得られる値をＸとする。残りのグループG_2とG_3、G_4とG_5についても、それぞれ、同様の処理を行う。これらによって得られる値をＹ，Ｚとする。こうして、基底空間Ｂの各点ごとに、３つの値Ｘ，Ｙ，Ｚが得られる。この様子を、図７に示す。なお、このグルーピングの仕方は、一例であり、何番目のフレームが何番目のグループに属するかを予め定めておけば、他のグルーピング方法によってももちろん構わない（様々なバリエーションが可能である）。

【００７５】

ここで、それら３つの値Ｘ，Ｙ，Ｚを、Ｘ成分、Ｙ成分、Ｚ成分とするように、空間Ｓ（色空間Ｃの中に対象空間Ｔを包含する所定の部分空間Ｓ）を構成する。

【００７６】

６つのグループにおいて、Ｂの各点ごとにｇ個のフレームの輝度値の和をとって得られるものを、$f_0, f_1, f_2, f_3, f_4, f_5$：Ｂ→［０，２５６ｇ）とすると、Ｘ成分、Ｙ成分、Ｚ成分は、それぞれ、f_0-f_1、f_2-f_3、f_4-f_5で与えられる。f_0-f_1、f_2-f_3、f_4-f_5を、輝度差分値と総称するものとする。

【００７７】

空間Ｓの座標（Ｘ，Ｙ，Ｚ）は、Ｘ∈［－２５６ｇ，２５６ｇ）、Ｙ∈［－２５６ｇ，２５６ｇ）、Ｚ∈［－２５６ｇ，２５６ｇ）である（厳密には、［－２５５ｇ，２５５ｇ］内にある）。

【００７８】

空間Ｓの中に、半径εの２次元球面S^2をとり、これを対象空間Ｔとする。

【００７９】

対象空間Ｔ上の座標としてＨ、極座標（Θ，Φ）をとる。Θ∈［０，π）、Φ∈［０，２π）とする。対象空間Ｔ上の（Θ，Φ）は、空間Ｓ内の（Ｘ，Ｙ，Ｚ

）で表すと、

$$X=\sin\Theta\cdot\cos\Phi$$

$$Y=\sin\Theta\cdot\sin\Phi$$

$$Z=\cos\Theta$$

となる。

【００８０】

６ｇ枚の画像から得られる輝度差分値の画像を考えると、基底空間Ｂの各点において、対象空間Ｔ中の一点が割り当てられていることになる。この様子を、図８に表す。

【００８１】

このようにして、６ｇ枚の画像から得られる輝度差分値の画像は、S^2からS^2への写像として定義される。

【００８２】

この場合、電子透かしとして利用するホモトピー類は、２次元球面Ｂ＝S^2から２次元球面Ｔ＝S^2への写像の間のホモトピー同値に関する同値類$\pi^2(S^2)$である。$\pi^2(S^2)$==ZZであることが知られている。ここで、ZZは、有理整数の集合である。また、==は、「群としての同型」を意味するものとする。よって、電子透かしは、整数値によって与えられる。そこで、このホモトピー群の元が透かし情報を表現するように、画像を変更することで、透かし情報の埋め込みを行うことが可能である。

【００８３】

例えば、図６の画像の左上を原点にとると、ホモトピー類ｂ＝１の場合には、該画像の外周（端部）が２次元球面の（０，０，１）すなわち北極にあたる部分に対応し、該画像の中心が２次元球面の（０，０，－１）すなわち南極にあたる部分に対応し、その間は、連続的に対応することになる。すなわち、図６の基底空間での赤道周りでの１周が、図８の対象空間での赤道周りでの１周に対応する。

【００８４】

この様子を、図９～図１２に示す。各図において、（ａ）は画像上の位置のう

ち２次元球面の基底空間におけるある経線に対応する部分を両矢印で示し、（ｂ），（ｃ）は（ａ）で示された部分に埋め込まれている値が示す対象空間における位置を示す。また、（ｂ）は対象空間を北極側からみた様子を示し、（ｃ）は対象空間を赤道側からみた様子を示している。

【００８５】

なお、ホモトピー類ｂ＝－１の場合にも、同様であるが、対象空間での赤道周りでの１周が、ｂ＝１の場合に比べて逆回りになる。また、ｂ＝２または－２の場合には、基底空間での赤道周りでの１周が、対象空間での赤道周りでの２周に対応する。

【００８６】

本具体例では、各画素の輝度差分値が、上記のようにホモトピー類ｂに応じた対応を与えるように、画素値の変更を行うことによって、ホモトピー類ｂの埋め込みを行えばよい。

【００８７】

ただし、詳しくは後述するが、本実施形態では、画像への電子透かしの埋め込みを行う前に、各画素へ埋め込むべき値に対する鍵情報に基づく掻き混ぜを行う。すなわち、図１３に示すように、（ａ）のような画像の本来の各画素位置に、各埋め込み値を埋め込む前に、（ｂ）のように掻き混ぜを行って、埋め込む。この状態では、同じアルゴリズムを用いても、基底空間での赤道周りでの１周が、対象空間ではランダムな遷移を示すだけであり、意味のある情報を得ることはできない（正しいホモトピー類すなわち電子透かしを求めることができないばかりでなく、電子透かしの存在自体が分からない）。埋め込み時に用いられた鍵情報に対応する鍵情報があってはじめて、図１４に示すように、掻き混ぜ戻しを行って、画像の本来の各画素位置に対応する各埋め込み値を検出することができ、正しいホモトピー類すなわち電子透かしを求めることができる。

【００８８】

このように、電子透かしのアルゴリズムが開示されたとしても鍵情報が開示されていなければ安全であるように構成することができるようにしている。

【００８９】

図１５に、本具体例の場合の電子透かし埋込装置における処理手順の一例を示す。

【００９０】

まず、最初に、電子透かし埋込装置には、電子透かしを埋め込む対象となる埋め込み対象画像と、埋め込むべき透かし情報であるホモトピー類と、鍵情報とが与えられる。

【００９１】

次に、関数生成部１１は、与えられたホモトピー類に属する関数を生成する。

【００９２】

関数生成部１１の具体例を説明する。

【００９３】

関数生成部１１は、Ｘ成分生成部とＹ成分生成部とＺ成分生成部とを含む（図示せず）。関数の形には、種々のバリエーションがあるが、一例として、次のようなものがある。

$$\Theta = \theta \qquad (1)$$

$$\Phi = b\phi \quad (\mathrm{mod}\ 2\pi) \qquad (2)$$

ここで、ｂは、電子透かしであるのもトピー類であって、$b \in ZZ == \pi^2(S^2)$である。

【００９４】

なお、あるホモトピー類に属する関数として、上記式以外のものを選択してもよい。周期的ではない関数でもよい。

【００９５】

また、予め用意された複数の異なる関数をそれぞれ用いてコンテンツに対する位相不変量の設定を行ったとした場合に対象コンテンツの内容に与える影響を評価し、対象コンテンツの内容に与える影響を最小にすると評価される関数を選択するようにしてもよい。

【００９６】

ところで、対象空間Ｔ上の点に対応する座標（Ｘ，Ｙ，Ｚ）の値は、座標（Θ，Φ）の値の関数であり、上記式より、座標（Θ，Φ）の値は、基底空間Ｂと同

一視されたＳ^{2}上の座標（θ，ϕ）の値の関数である。基底空間Ｂ上の各点に対する（Ｘ，Ｙ，Ｚ）の値の計算は、この座標変換を表す式中に現れる初等的な関数を計算する機能を組み合わせて用いることで実現できる。初等的な関数の計算は、例えば、その関数の入力と出力の対応をテーブルとして持つことにより実現できる。

【００９７】

こうして、関数生成部１１は、電子透かし情報ｂ∈ZZの入力に対して、Ｂの各点に対して、対応する（Ｘ，Ｙ，Ｚ）の値を出力する。

【００９８】

次に、掻き混ぜ関数生成部１１は、与えられた鍵情報に従って、掻き混ぜ関数を生成し、関数生成部１１が生成した関数との合成関数を計算する。

【００９９】

関数掻き混ぜ部１２の具体例を説明する。

【０１００】

関数掻き混ぜ部１２は、鍵情報ｋの入力に対して、掻き混ぜ関数を生成する。

【０１０１】

掻き混ぜ関数は、ＳからＳへの写像であって、鍵情報の値により異なる写像となるものである。

【０１０２】

以下、その一例を示す。

【０１０３】

空間Ｓの各座標を、それぞれ、２５６のブロックに分割する。

【０１０４】

座標ごとにブロックを指定するためには、８ビットあればよいので、３つの座標（Ｘ，Ｙ，Ｚ）のすべてでブロックを指定するには、２４ビットあればよい。この（Ｘ，Ｙ，Ｚ）を表す２４ビットの情報が指定されると、空間Ｓ中のある一区画が特定される。ここでは、これらの区画の間の置換を鍵情報に依存して生成する。そのためには、２４ビットの情報が入力されると、２４ビットの情報を出力する全単射の関数を鍵依存となるように構成できればよい。このために、本例

では、ブロック暗号の構成方法を用いる。

【０１０５】

ブロック暗号の構成方法の１つがＦｅｉｓｔｅｌ網を利用する方法であり、ＤＥＳがその例である。

【０１０６】

ここでは、Ｆｅｉｓｔｅｌ網を利用して図１６に例示するような構成を用いる。

【０１０７】

図１６中、１２１は、排他的論理和である。１２２の部分の内部構成において、１２２１はＳ－ｂｏｘ、１２２２は排他的論理和である。Ｓ－ｂｏｘは、８入力８出力の全単射関数で、ランダムな変換を行う。ｒ回同じ操作を繰り返すことで、入力と出力は、ランダムな関係となる。k_1～k_rは、鍵情報である。この場合、鍵情報ｋは、k_1～k_rの合わせて８ｒビットの長さとなる。掻き混ぜ関数g_kは、この区間の置き換えとする。

【０１０８】

図１６の構成の上部から、関数生成部１１が生成した関数値が入力され、図１６の構成の下部から、それが掻き混ぜ関数と合成された結果の関数値が出力される。

【０１０９】

関数掻き混ぜ部１２は、関数生成部１１から得た基底空間Ｂから対象空間Ｔへの関数Ψ_bに対して、Ｓ⊃Ｔに対して、生成したＳからＳへの掻き混ぜ関数g_kを適用し、基底空間ＢからＳ内への関数$g_k \circ \Psi_b$を生成する。これは、関数生成部１１が与えられた基底空間Ｂの各点に対応する対象空間Ｔ上の点を、さらに、掻き混ぜ関数の対応関係に従って、Ｓ内の点に写すことによって行われる。

【０１１０】

なお、上記では、Ｘ成分とＹ成分とＺ成分をまとめて同一の掻き混ぜ関数を適用したが、その代わりに、Ｘ成分とＹ成分とＺ成分とに対して異なる掻き混ぜ関数を個別に適用するようにしてもよい。この場合には、後述する、掻き混ぜ戻しにおいては、Ｘ成分とＹ成分とＺ成分とのそれぞれについて当該掻き混ぜ関数に

対応する掻き混ぜ戻し関数を個別に適用することになる。

【０１１１】

次に、合成関数のＸ成分、Ｙ成分、Ｚ成分の各成分は、それぞれ、ｇ個のフレームからなるグループ２つに対して埋め込まれる。最後に、電子透かしが埋め込まれた埋め込み済み画像が出力される。

【０１１２】

関数埋め込み部１３の具体例を説明する。

【０１１３】

関数埋め込み部１３は、関数掻き混ぜ部１２が出力した合成関数$g_k \bigcirc \Psi_b$：Ｂ→Ｓを埋め込み対象画像に埋め込む。

【０１１４】

前述したように、６ｇ枚のフレームを６つのグループG_0～G_5に分け、Ｘ成分、Ｙ成分、Ｚ成分に対応する２つのグループG_0とG_1，G_2とG_3，G_4とG_5に対して、それぞれ、次のように、合成関数のＸ成分、Ｙ成分、Ｚ成分の埋め込みを行う。

［Ｘ成分］

グループG_0　：　$f_0 \rightarrow f_0 + (\varepsilon/2)[g_k \bigcirc \Psi_b]_x$

グループG_1　：　$f_1 \rightarrow f_1 - (\varepsilon/2)[g_k \bigcirc \Psi_b]_x$

［Ｙ成分］

グループG_2　：　$f_2 \rightarrow f_2 + (\varepsilon/2)[g_k \bigcirc \Psi_b]_y$

グループG_3　：　$f_3 \rightarrow f_3 - (\varepsilon/2)[g_k \bigcirc \Psi_b]_y$

［Ｚ成分］

グループG_4　：　$f_4 \rightarrow f_4 + (\varepsilon/2)[g_k \bigcirc \Psi_b]_z$

グループG_5　：　$f_5 \rightarrow f_5 - (\varepsilon/2)[g_k \bigcirc \Psi_b]_z$

例えば、Ｘ成分について、埋め込み前に検出されるグループG_0の輝度差分値がf_0であったならば、埋め込み後に検出されることになる輝度差分値が$f_0 + (\varepsilon/2)[g_k \bigcirc \Psi_b]X$　となるように、各フレームの画素の画素値を変更することによって、埋め込みを行う。

【０１１５】

なお、各ｆ$_i$への埋め込みは、そのグループに属するｇ枚のフレームに対して均等に埋め込みを行ってもよいし、フレーム毎に、埋め込む強さを変えてもよい。さらに、均等に埋め込むか、埋め込む強さを変えるかを、Ｂの点毎に、決めてもよい。また、フレーム毎の埋め込む強さの変え方もＢの点毎に変えてもよい。

【０１１６】

また、実際に透かし情報の埋め込みに用いるのは、画素値の全ビットではなく、そのうち、ノイズの影響を受けにくく、かつ、画像の画質に大きな影響を与えない、予め定められた特定の中間のビットプレーンの領域（通常は連続する複数ビット）を用いるようにしてもよい。

【０１１７】

図１７に、本具体例の場合の電子透かし検出装置における処理手順の一例を示す。

【０１１８】

まず、最初に、電子透かし検出装置には、電子透かしを検出する対象となる検出対象画像と、電子透かしの埋め込みに用いられた鍵情報が与えられる。

【０１１９】

次に、関数検出部２１は、埋め込まれている関数のＸ成分、Ｙ成分、Ｚ成分をそれぞれｇ個のフレームからなる２つのグループから抽出する。

【０１２０】

関数検出部２１の具体例を説明する。

【０１２１】

関数検出部２１は、６ｇ個のフレームから、図７のように、Ｘ成分、Ｙ成分、Ｚ成分を計算する。なお、埋め込みの際には、εという定数を掛けて埋め込んでいたので、検出の際には、検出された成分値に１／εを掛けておく。

【０１２２】

こうして、関数Φ：Ｂ→Ｓが求まる。

【０１２３】

関数の表現方法の例としては、基底空間Ｂの点ごとに、関数値を対応付けたリストとして表す方法がある。

【０１２４】

次に、関数掻き混ぜ戻し部２２は、与えられた鍵情報に従って、掻き混ぜ戻し関数を生成し、関数検出部２１が抽出した関数との合成関数を計算する。

【０１２５】

関数掻き混ぜ戻し部２２は、与えられた鍵情報ｋに従って、掻き混ぜ戻し関数を生成する。この掻き混ぜ戻し関数は、埋め込みの際に用いた鍵と同じ鍵が与えられた場合には、掻き混ぜ関数の逆関数となっている。

【０１２６】

関数掻き混ぜ部１２においては、Ｆｅｉｓｔｅｌ網を利用して図１６のような構成で掻き混ぜ関数を実現したが、その逆関数は、図１８に例示するような構成で実現できる。

【０１２７】

図１８中、２２１は、排他的論理和である。２２２の部分の内部構成において、２２２１はＳ－ｂｏｘ、２２２２は排他的論理和である。k_1～k_rは、鍵情報である。

【０１２８】

図１８の構成の上部から、関数検出部２１が抽出した関数値が入力され、図１８の構成の下部から、それが掻き混ぜ戻し関数と合成された結果の関数値が出力される。

【０１２９】

次に、ホモトピー類計算部２３は、得られた合成関数から、ホモトピー類を計算する。最後に、計算されたホモトピー類が電子透かしとして出力される。

【０１３０】

ホモトピー類計算部２は、関数掻き混ぜ戻し部２２によって計算された合成関数から、ホモトピー類を計算する。

【０１３１】

関数掻き混ぜ戻し部２２の計算した合成関数を、

$$ff=(X, Y, Z)=(\sin\Theta\cdot\cos\Phi, \sin\Theta\cdot\sin\Phi, \cos\Theta)$$

で表す。

【０１３２】

関数掻き混ぜ戻し部２２に埋め込みの際に用いた鍵と同じ鍵が与えられた場合には、この合成関数は、電子透かし埋込装置の関数生成部１１が生成した、電子透かしとして与えられたホモトピー類ｂに属する関数（Ψ_b：Ｂ→Ｔ）である。

【０１３３】

この合成関数のホモトピー類ｂ(ff)は、

$$b(ff)=(1/4\pi)\int_0^{2\pi}d\theta\int_0^{\pi}d\phi\ ff\cdot\partial ff/\partial\theta\times\partial ff/\partial\phi$$

で計算される。ここで、θ，ϕは、基底空間Ｂと同一視された2次元球面S^2上の座標である。また、ベクトル演算において、・と×は、それぞれ、Ｘ座標、Ｙ座標、Ｚ座標を正規直交するとみなしたときの、空間Ｓ内での内積と外積である。なお、$\int_0^{2\pi}$の0と2πは積分の範囲が0～2πであることを示している。

【０１３４】

もとの基底空間Ｂ上の積分で表すと、ホモトピー類ｂ(ff)は、

$$b(ff)=(1/4\pi)\int_0^{W}d\theta\int_0^{H}dy\ ff\cdot\partial ff/\partial x\times\partial ff/\partial y$$

となる。

【０１３５】

実際の画像において、Ｂは離散空間であるから、上記式における積分は和によって置き換えられ、微分は差分によって置き換えて行われる。この場合、ホモトピー類ｂ（ff）は、

$$b\ (ff)=(1/4\pi WH)\Sigma_{x=0}^{W-1}\Sigma_{y=0}^{H-1}\ ff\cdot\Delta_x ff\times\Delta_y ff \qquad (3)$$

となる。

【０１３６】

ここで、

$\Delta_x ff(x,y)=ff(x+1,y)-ff(x,y)$　（ｘ≠Ｗ－１のとき）

$\Delta_x ff(x,y)=ff(0,y)-ff(W-1,y)$　（ｘ＝Ｗ－１のとき）

$\Delta_y ff(x,y)=ff(x,y+1)-ff(x,y)$　（ｘ≠Ｈ－１のとき）

$\Delta_y ff(x,y)=ff(x,0)-ff(x,H-1)$　（ｘ＝Ｈ－１のとき）

である。

なお、$\Sigma_{x=0}^{W-1}$のx=0とW-1は総和の範囲がx=0～W-1であることを示している。

【０１３７】

最終的には、この計算結果に最も近い整数値を電子透かしの値として出力する。

【０１３８】

図１９に、ホモトピー類計算部２３の構成例を示す。

【０１３９】

第１の微分計算部２３１は、上記のｘ方向の微分（差分）を計算し、第２の微分計算部２３２は、上記のｙ方向の微分（差分）を計算する。外積計算部２３３は、これら２つの微分（差分）の外積を計算し、内積計算部２３４は、この内積結果と、もとの関数を内積する。最後に、積分計算部２３５は、この内積結果を基底空間Ｂに渡って積分し、必要に応じて、整数値への丸めを行う。

【０１４０】

ところで、上記具体例では、６ｇ枚のフレームをもとに処理を行ったが、例えば、４つのフレームを縦横に接続してこれを処理上の１フレームとみなして処理する方法（この場合、２４ｇ枚のフレームをもとに処理することになる）や、１つのフレームを縦横に分割してこれを処理上の４つの連続するフレームとみなして処理する方法（この場合、６ｇ／４枚のフレームをもとに処理することになる）なども可能である。

【０１４１】

また、上記具体例では、濃淡画像を例にとって説明したが、本実施形態は、もちろん、カラー画像にも適用可能である。この場合には、例えば、最初のｇ枚の画素の色のＹ成分をグループG_0、次のｇ枚の画素の色のＹ成分をグループG_1、最初のｇ枚の画素の色のＵ成分をグループG_2、次のｇ枚の画素の色のＵ成分をグループG_3、最初のｇ枚の画素の色のＶ成分をグループG_4、次のｇ枚の画素の色のＶ成分をグループG_5として、同様の処理を行えばよい。また、Ｙ成分のみを用いるものとして、同様の処理を行うことも可能である。その他にも、種々のバリエーションが可能である。もちろん、カラー画像においても、何番目のフレームのどの成分が何番目のグループに属するかを予め定めておけば、どのようなグルーピングの仕方によっても構わない（様々なバリエーションが可能である）

。

【０１４２】

また、上記具体例では、動画像を例にとって説明したが、本実施形態は、静止画にも適用可能である。この場合には、例えば、静止画を６ｇ個に分割して、分割部分のそれぞれを処理上の１フレームとみなして処理するようにしてもよい。

【０１４３】

また、上記具体例では、隣接する２つの（例えばｇ枚の画素からなる）グループの画素値に関する差分値を利用して、電子透かしを埋め込むようにしたが、１つの（例えばｇ枚の画素からなる）グループに直接電子透かしを埋め込など、種々の方法が可能である。

【０１４４】

また、これまで本実施形態で説明した埋め込み方は、一例であり、他の異なる埋め込み方法も可能である。

【０１４５】

以下では、本実施形態のさらなるバリエーションについて詳しく説明する。

【０１４６】

まず、これまで各構成例では、基底空間をS^2、対象空間をS^2として説明したが、それぞれ、非自明なトポロジーを持つ基底空間や対象空間を用いる場合など、他の空間を採用することによる実現形態も可能である。

【０１４７】

例えば、画像の上端と下端とを同一視し、右端と左端とを同一視することで、基底空間をトーラスT^2とすることも可能である。

【０１４８】

次に、埋め込み画像を表す関数のバリエーションについて説明する。

【０１４９】

埋め込み画像を表す関数において、画像周辺近傍での関数の変化を緩やかにし、周辺に近づくにつれ一定の値に漸近的に近づくように取れば、画像の切り取りが画像の中央付近の切り取りである場合には、失われた周辺部の積分値への影響は小さい。したがって、画像の中央付近に重要な内容が集中したコンテンツの場

合には（そのようなコンテンツは比較的多いと考えられる）、切り取りに対する耐性もある程度実現できる。一般的には、その画像の重要な部分において関数の変化が大きくなるようにすれば、重要な部分だけを切り抜いても電子透かしが残るようにできる。

【０１５０】

次に、音声データに対する処理のバリエーションについて説明する。

【０１５１】

これまでは、対象コンテンツとして画像を例にとって説明してきたが、本実施形態は、他のメディアのデジタルコンテンツに対しても適用可能である。例えば、音声や音楽のデジタルコンテンツについては、特開２００２－１４２０９４に開示された方法を用いればよい。

【０１５２】

次に、位相不変量のバリエーションについて説明する。

【０１５３】

本実施形態では、位相不変量としてホモトピー類を用いて説明してきたが、それ以外の位相不変量を用いることも可能である。

【０１５４】

ホモトピー群（の元）以外の不変量（ｉｎｖａｒｉａｎｔ）としては、例えば、ホモロジー群、コホモロジー群、あるいは、ベクトル束におけるＳｔｉｅｆｅｌ－Ｗｈｉｔｎｅｙ類、Ｃｈｅｒｎ類、Ｐｏｎｔｒｙａｇｉｎ類といった特性類（ｃｈａｒａｃｔｅｒｉｓｔｉｃ　ｃｌａｓｓ）、多様体のＥｕｌｅｒ数、指数（ｉｎｄｅｘ）や符号数（ｓｉｇｎａｔｕｒｅ）、結び糸に関するＡｌｅｘａｎｄｅｒ不変量、あるいは、絡み糸に関するＭｉｌｎｏｒ不変量など、多数のものが知られており（例えば、岩波数学事典第３版，日本数学会編集，岩波書店）、それら不変量を用いることも可能である。

【０１５５】

なお、ホモトピー群では、例えば、Ｇａｕｓｓ－Ｂｏｎｎｅｔの定理によって与えられる積分を用いたが、Ｃｈｅｒｎ類などの特性類の場合には、例えば、Ａｔｉｙａｈ－Ｓｉｎｇｅｒの指数定理が与える積分を用いることができる。それ

らの場合、ホモトピー群について例示した積分量の代わりに、それらの不変量を導き出す積分量を用いればよい。

【０１５６】

以下では、本実施形態のハードウェア構成、ソフトウェア構成について説明する。

【０１５７】

本実施形態の電子透かし埋込装置は、ハードウェアとしても、ソフトウェア（（コンピュータに所定の手段を実行させるための、あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラム）としても、実現可能である。また、電子透かし埋込装置をソフトウェアで実現する場合には、記録媒体によってプログラムを受け渡しすることも、通信媒体によってプログラムを受け渡しすることもできる。もちろん、それらは、電子透かし検出装置についても同様である。

また、電子透かし埋込装置や電子透かし検出装置をハードウェアとして構成する場合、半導体装置として形成することができる。

また、本発明を適用した電子透かし埋込装置を構成する場合、あるいは電子透かし埋め込みプログラムを作成する場合に、同一構成を有するブロックもしくはモジュールがあっても、それらをすべて個別に作成することも可能であるが、同一構成を有するブロックもしくはモジュールについては１または適当数のみ用意しておいて、それをアルゴリズムの各部分で共有する（使い回す）ことも可能である。電子透かし検出装置を構成する場合、あるいは電子透かし検出プログラムを作成する場合も、同様である。また、電子透かし埋込装置および電子透かし検出装置を含むシステムを構成する場合、あるいは電子透かし埋め込みプログラムおよび電子透かし検出プログラムを含むシステムを作成する場合には、電子透かし埋込装置（あるいはプログラム）と電子透かし検出装置（あるいはプログラム）に渡って、同一構成を有するブロックもしくはモジュールについては１または適当数のみ用意しておいて、それをアルゴリズムの各部分で共有する（使い回す）ことも可能である。

【０１５８】

また、電子透かし埋込装置や電子透かし検出装置をソフトウェアで構成する場合には、マルチプロセッサを利用し、並列処理を行って、処理を高速化することも可能である。

【０１５９】

なお、この発明の実施の形態で例示した構成は一例であって、それ以外の構成を排除する趣旨のものではなく、例示した構成の一部を他のもので置き換えたり、例示した構成の一部を省いたり、例示した構成に別の機能あるいは要素を付加したり、それらを組み合わせたりすることなどによって得られる別の構成も可能である。また、例示した構成と論理的に等価な別の構成、例示した構成と論理的に等価な部分を含む別の構成、例示した構成の要部と論理的に等価な別の構成なども可能である。また、例示した構成と同一もしくは類似の目的を達成する別の構成、例示した構成と同一もしくは類似の効果を奏する別の構成なども可能である。

また、この発明の実施の形態で例示した各種構成部分についての各種バリエーションは、適宜組み合わせて実施することが可能である。

また、この発明の実施の形態は、個別装置としての発明、関連を持つ２以上の装置についての発明、システム全体としての発明、個別装置内部の構成部分についての発明、またはそれらに対応する方法の発明等、種々の観点、段階、概念またはカテゴリに係る発明を包含・内在するものである。

従って、この発明の実施の形態に開示した内容からは、例示した構成に限定されることなく発明を抽出することができるものである。

【０１６０】

本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【０１６１】

【発明の効果】

本発明によれば、ＳｔｉｒＭａｒｋ攻撃やＤ－Ａ－Ｄ－変換などの局所的変形に対する耐性を持つとともに、電子透かしのアルゴリズムの全部又は一部が開示されたとしてもなお安全であるような電子透かしを実現することができる。

【図面の簡単な説明】

【図１】　本発明の一実施形態に係る電子透かし埋込装置及び電子透かし検出装置を含むコンテンツ流通システムの概略構成を示す図

【図２】　同実施形態に係る電子透かし埋込装置の構成例を示す図

【図３】　同実施形態に係る電子透かし埋込装置の処理手順の一例を示すフローチャート

【図４】　同実施形態に係る電子透かし検出装置の構成例を示す図

【図５】　同実施形態に係る電子透かし検出装置の処理手順の一例を示すフローチャート

【図６】　同実施形態において基底空間を２次元球面と同一視する様子を説明するための図

【図７】　同実施形態において動画像を対象コンテンツとする場合の輝度差分値の計算方法の一例を説明するための図

【図８】　同実施形態における基底空間と対象空間との例を示す図

【図９】　同実施形態における基底空間での赤道周りでの１周と対象空間での赤道周りでの１周との対応を説明するための図

【図１０】　同実施形態における基底空間での赤道周りでの１周と対象空間での赤道周りでの１周との対応を説明するための図

【図１１】　同実施形態における基底空間での赤道周りでの１周と対象空間での赤道周りでの１周との対応を説明するための図

【図１２】　同実施形態における基底空間での赤道周りでの１周と対象空間での赤道周りでの１周との対応を説明するための図

【図１３】　同実施形態における鍵情報に基づく掻き混ぜについて説明するための図

【図１４】　同実施形態における鍵情報に基づく掻き混ぜ戻しについて説明するための図

【図１５】　同実施形態に係る電子透かし埋込装置の処理手順の一例を示すフローチャート

【図１６】　同実施形態に係る関数掻き混ぜ部の構成例を示す図

【図１７】　同実施形態に係る電子透かし検出装置の処理手順の一例を示すフローチャート

【図１８】　同実施形態に係る関数掻き混ぜ戻し部の構成例を示す図

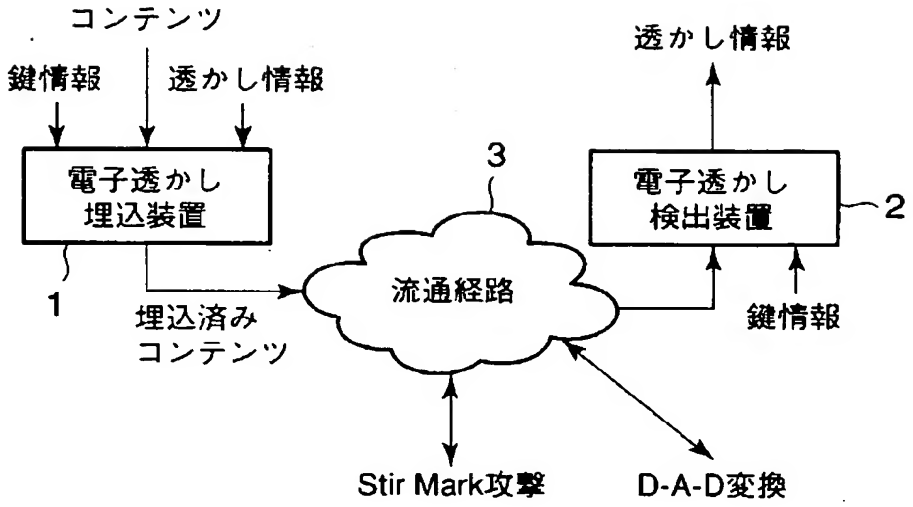
【図１９】　同実施形態に係るホモトピー類計算部の構成例を示す図

【符号の説明】

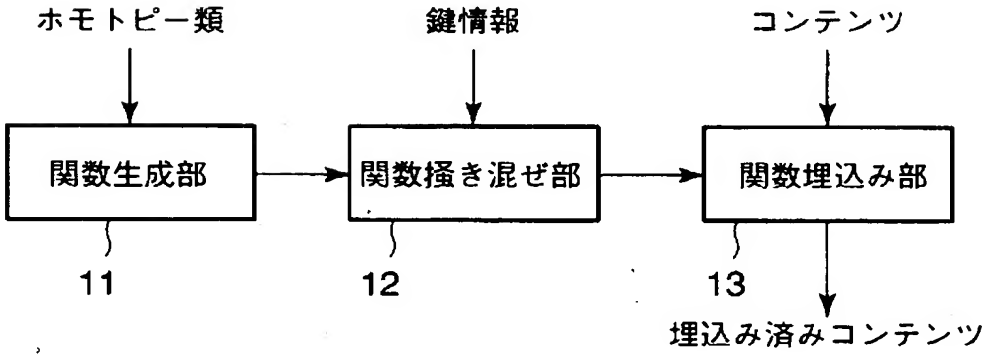
１…電子透かし埋込装置、２…電子透かし検出装置、３…流通経路、１１…関数生成部、１２…関数掻き混ぜ部、１３…関数埋め込み部、２１…関数検出部、２２…関数掻き混ぜ戻し部、２３…ホモトピー類計算部、１２１，１２２２，２２１，２２２２…排他的論理和、１２２１，２２２１…Ｓ－ｂｏｘ、２３１…第１の微分計算部、２３２…第２の微分計算部、２３３…外積計算部、２３４…内積計算部、２３５…積分計算部

【書類名】　図面

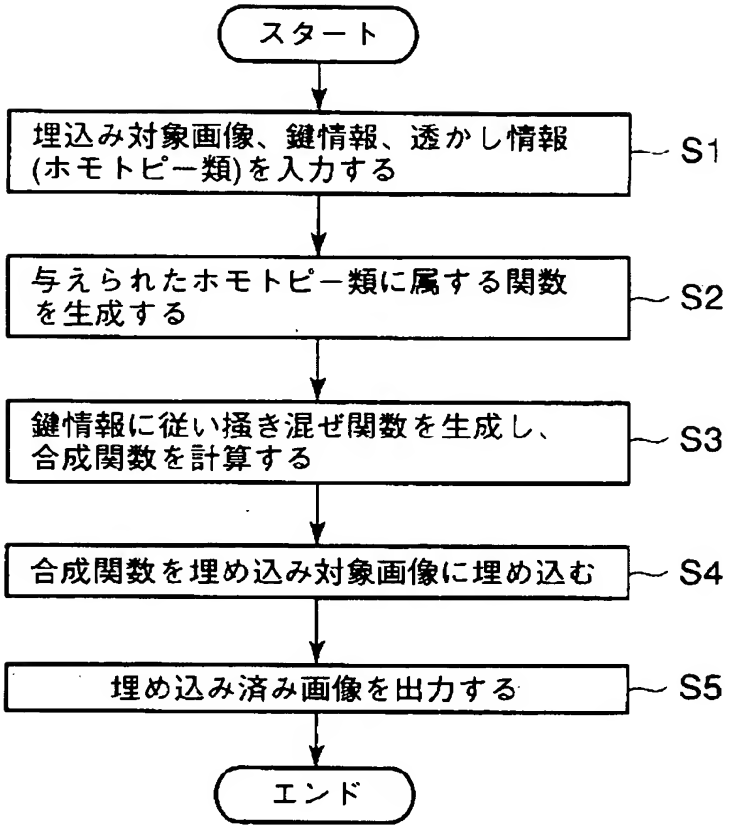
【図１】


コンテンツ
鍵情報
透かし情報
電子透かし
埋込装置
1
埋込済み
コンテンツ
3
流通経路
Stir Mark攻撃
D-A-D変換
透かし情報
電子透かし
検出装置
2
鍵情報

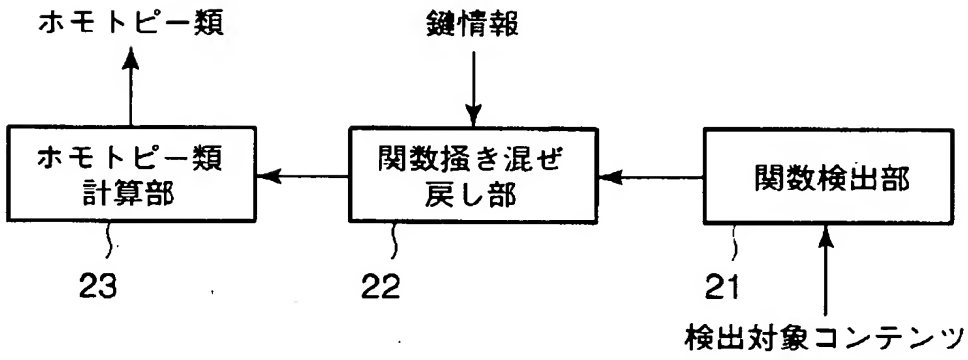
【図２】


ホモトピー類
鍵情報
コンテンツ
関数生成部
関数掻き混ぜ部
関数埋込み部
11
12
13
埋込み済みコンテンツ

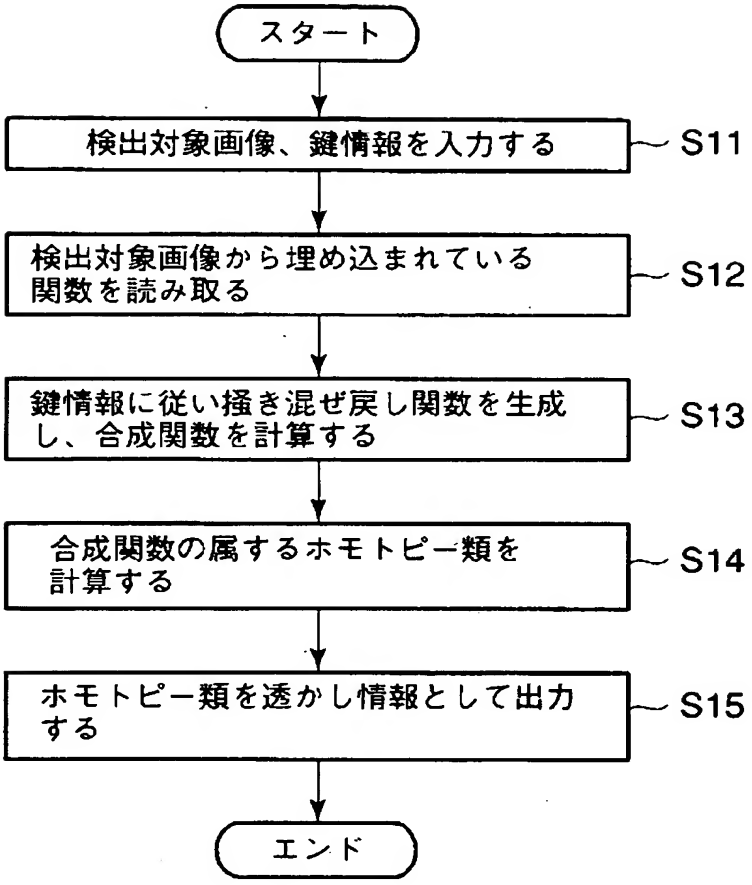
【図３】


スタート
埋込み対象画像、鍵情報、透かし情報
(ホモトピー類)を入力する
S1
与えられたホモトピー類に属する関数
を生成する
S2
鍵情報に従い掻き混ぜ関数を生成し、
合成関数を計算する
S3
合成関数を埋め込み対象画像に埋め込む
S4
埋め込み済み画像を出力する
S5
エンド

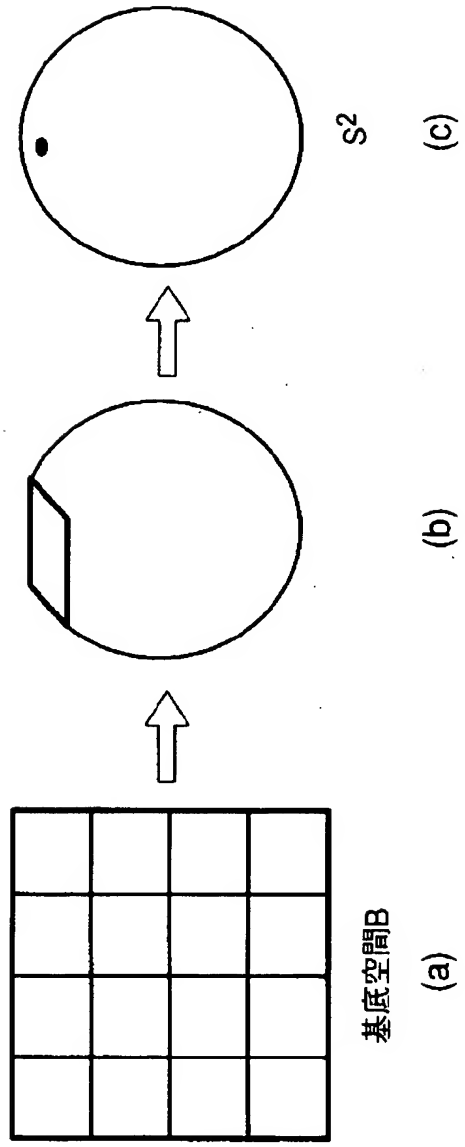
【図４】


ホモトピー類
鍵情報
ホモトピー類
計算部
関数掻き混ぜ
戻し部
関数検出部
23
22
21
検出対象コンテンツ

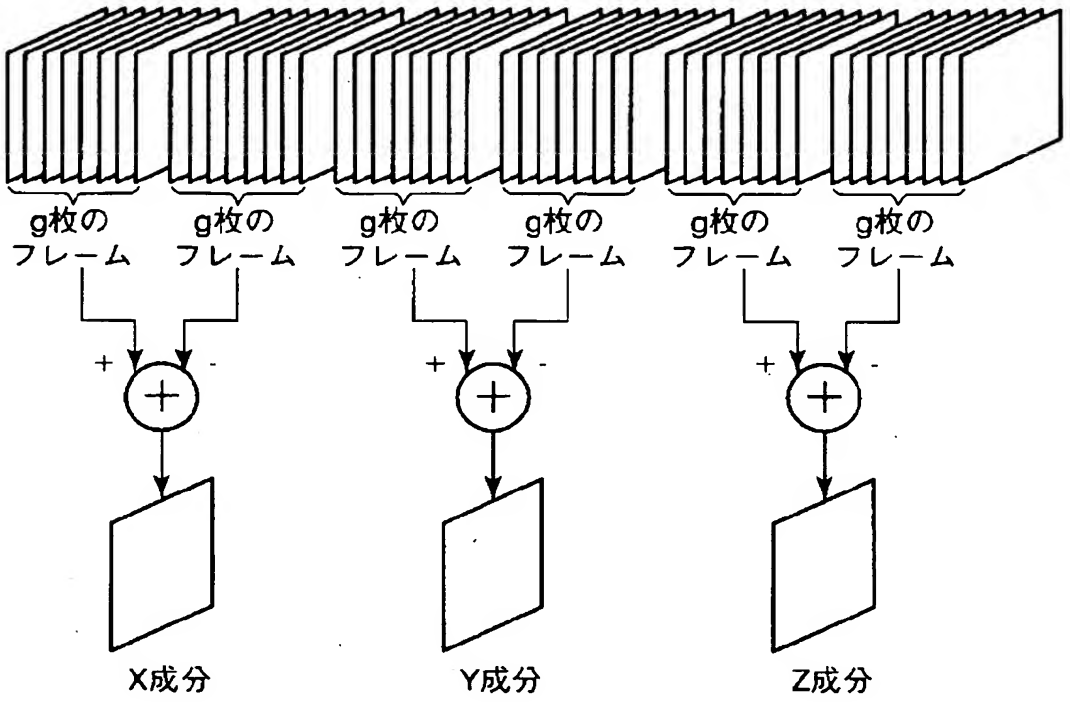
【図５】


スタート
検出対象画像、鍵情報を入力する
S11
検出対象画像から埋め込まれている関数を読み取る
S12
鍵情報に従い掻き混ぜ戻し関数を生成し、合成関数を計算する
S13
合成関数の属するホモトピー類を計算する
S14
ホモトピー類を透かし情報として出力する
S15
エンド

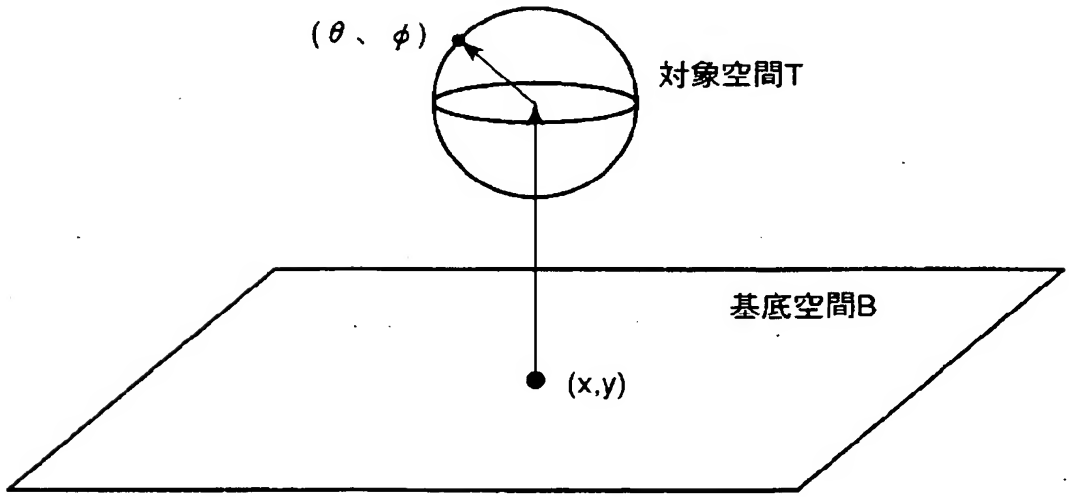
【図６】



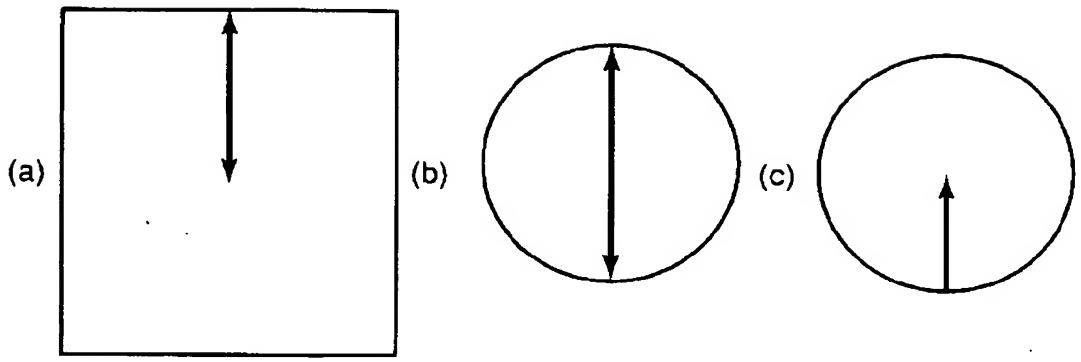
【図７】


g枚の
フレーム
g枚の
フレーム
g枚の
フレーム
g枚の
フレーム
g枚の
フレーム
g枚の
フレーム
+
-
+
-
+
-
X成分
Y成分
Z成分

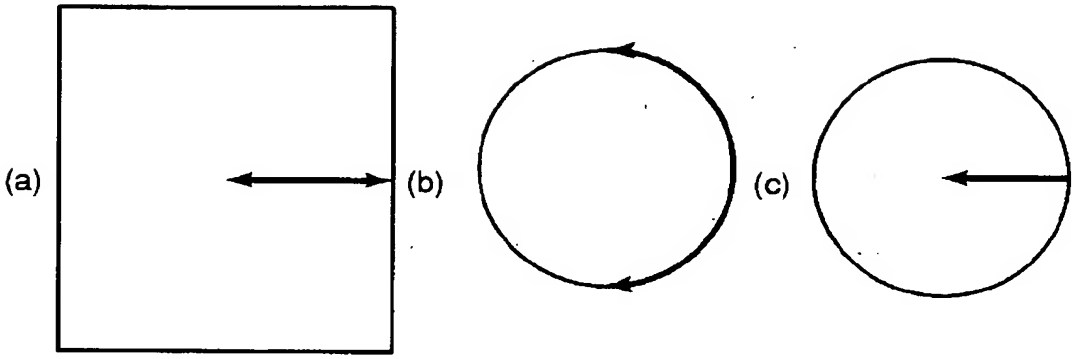
【図８】


(θ、φ)
対象空間T
基底空間B
(x,y)

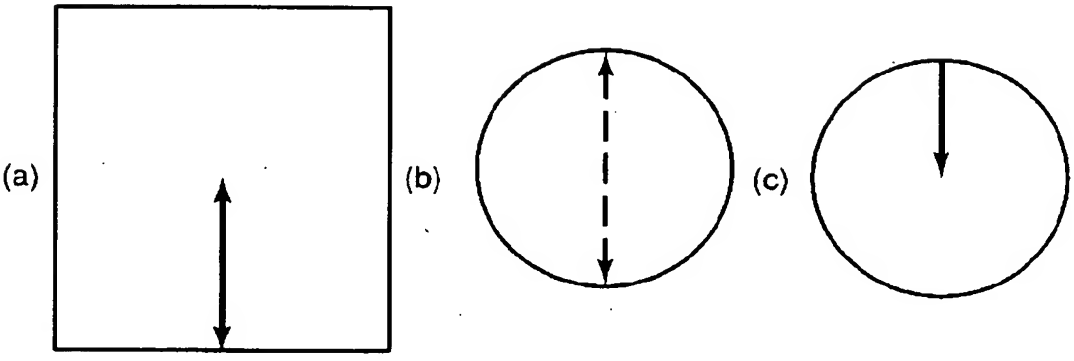
【図９】



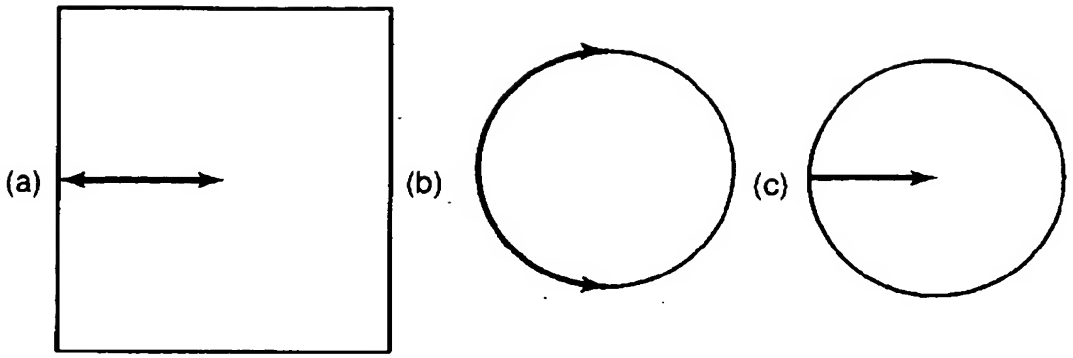
【図１０】



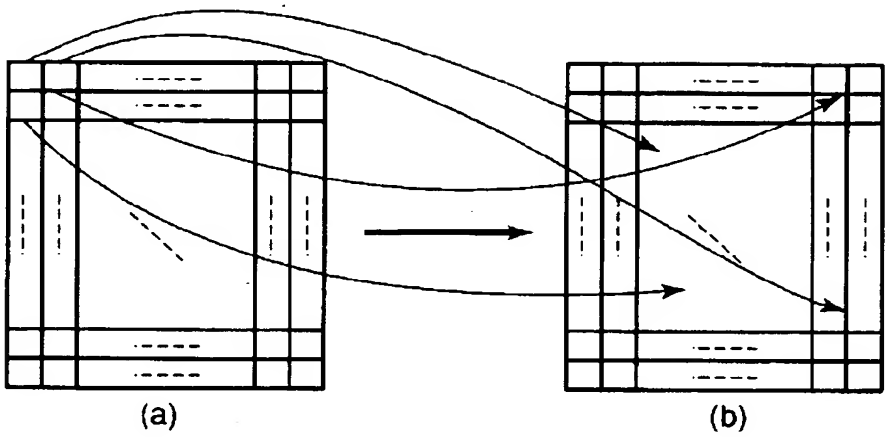
【図１１】



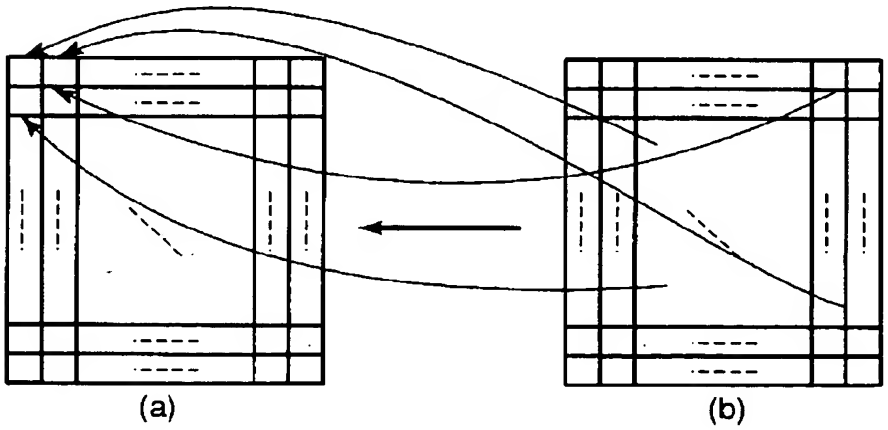
【図１２】



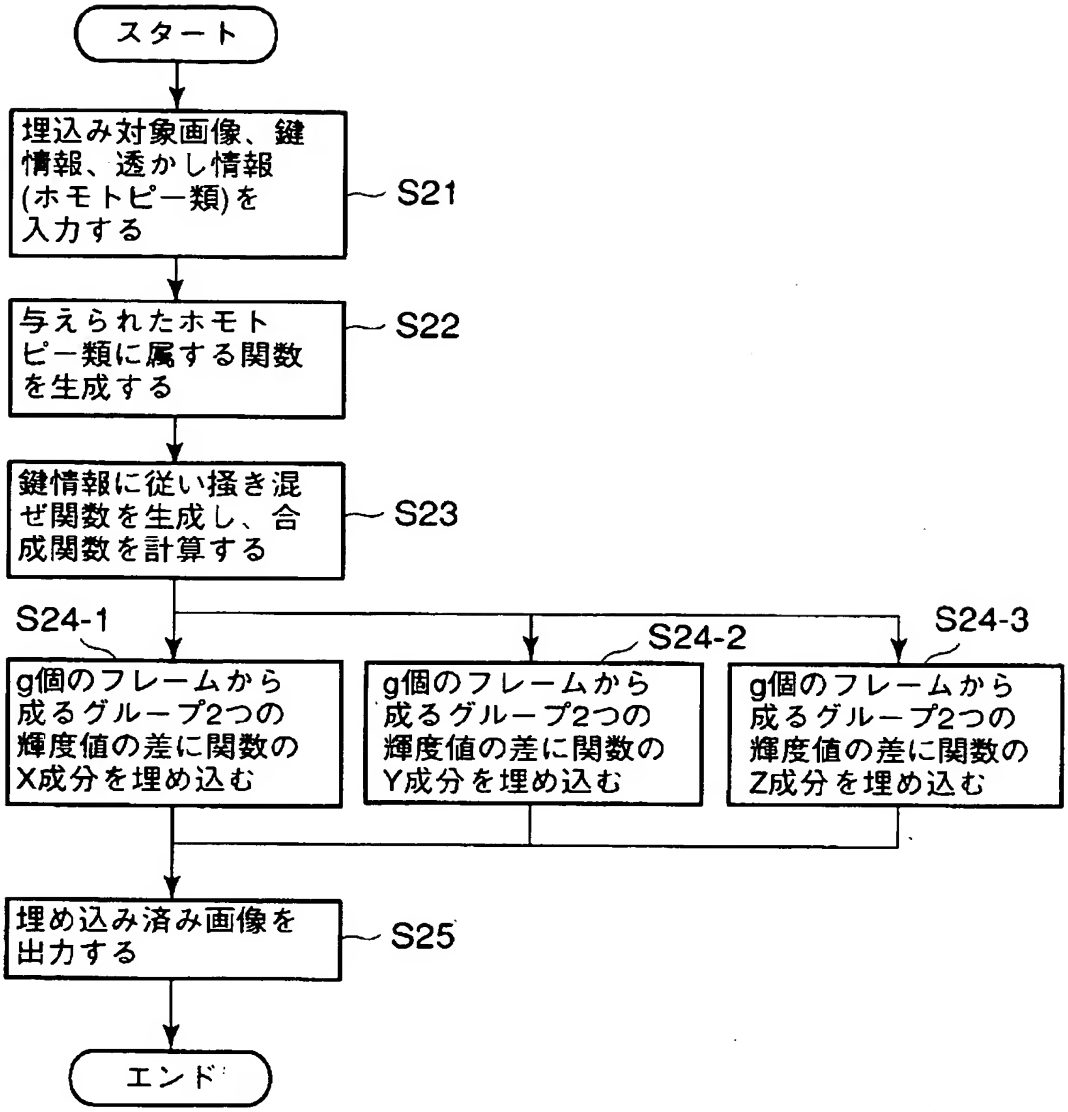
【図１３】



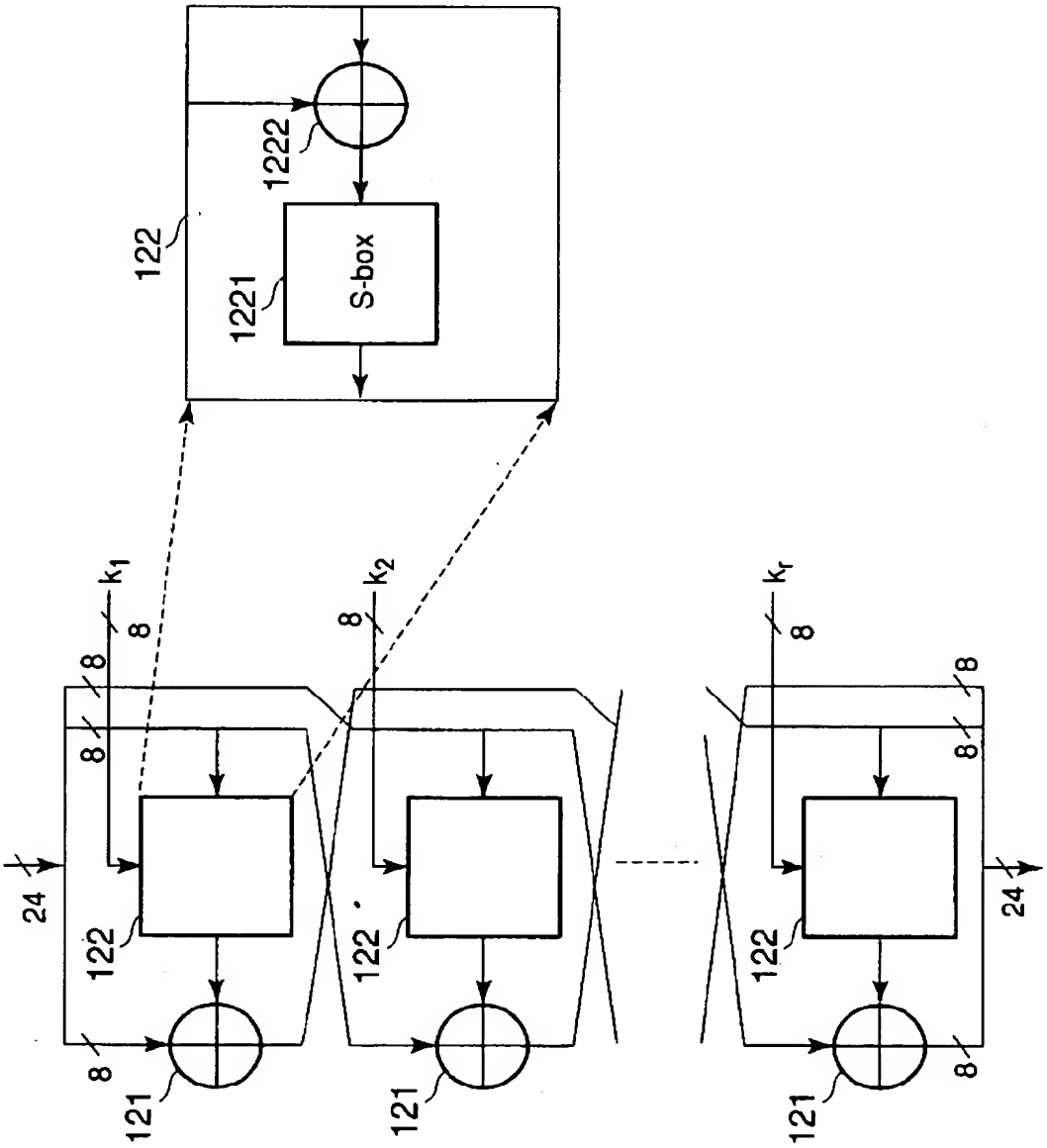
【図１４】



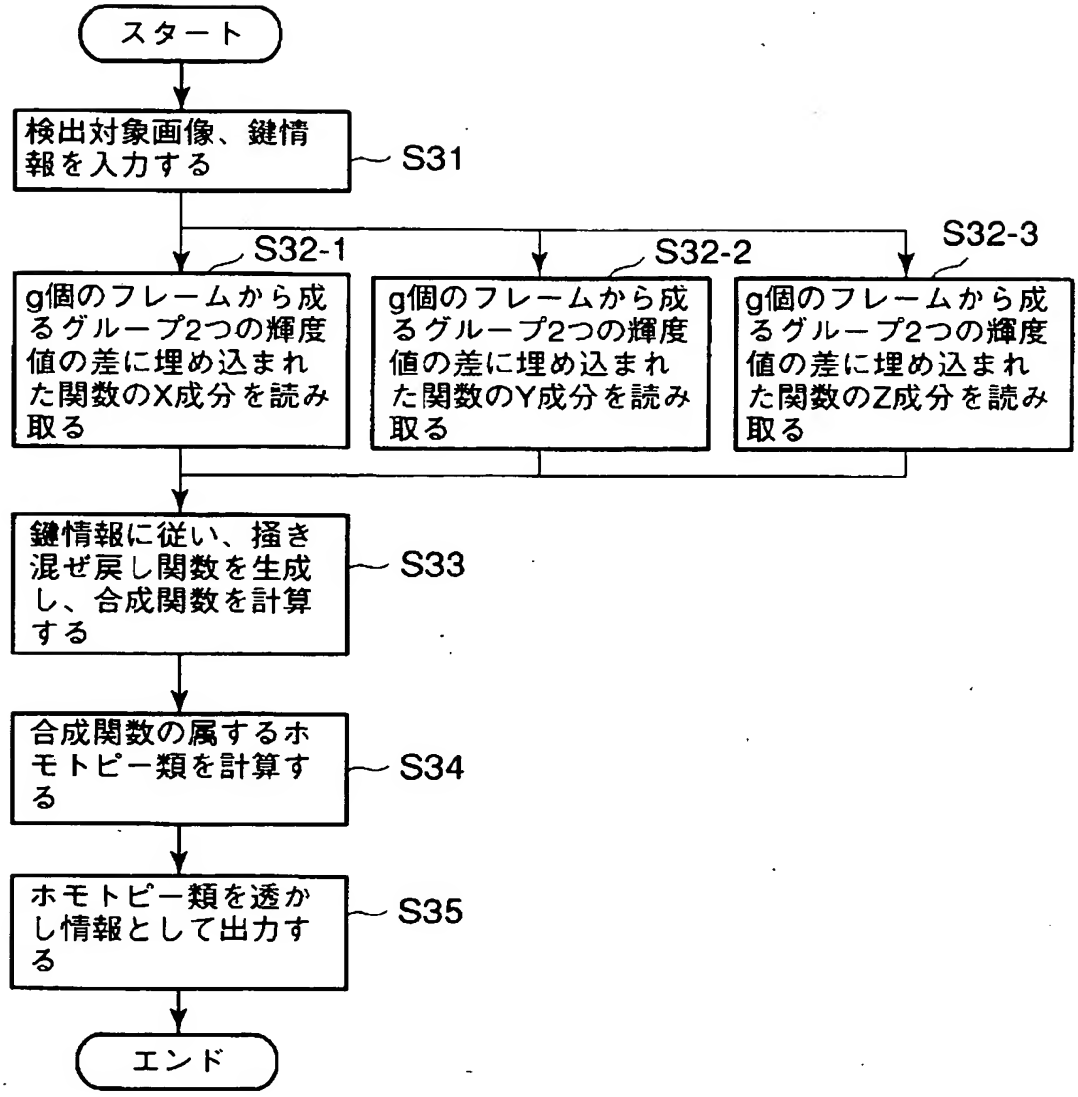
【図１５】


スタート
埋込み対象画像、鍵情報、透かし情報(ホモトピー類)を入力する
S21
与えられたホモトピー類に属する関数を生成する
S22
鍵情報に従い掻き混ぜ関数を生成し、合成関数を計算する
S23
S24-1
g個のフレームから成るグループ2つの輝度値の差に関数のX成分を埋め込む
S24-2
g個のフレームから成るグループ2つの輝度値の差に関数のY成分を埋め込む
S24-3
g個のフレームから成るグループ2つの輝度値の差に関数のZ成分を埋め込む
埋め込み済み画像を出力する
S25
エンド

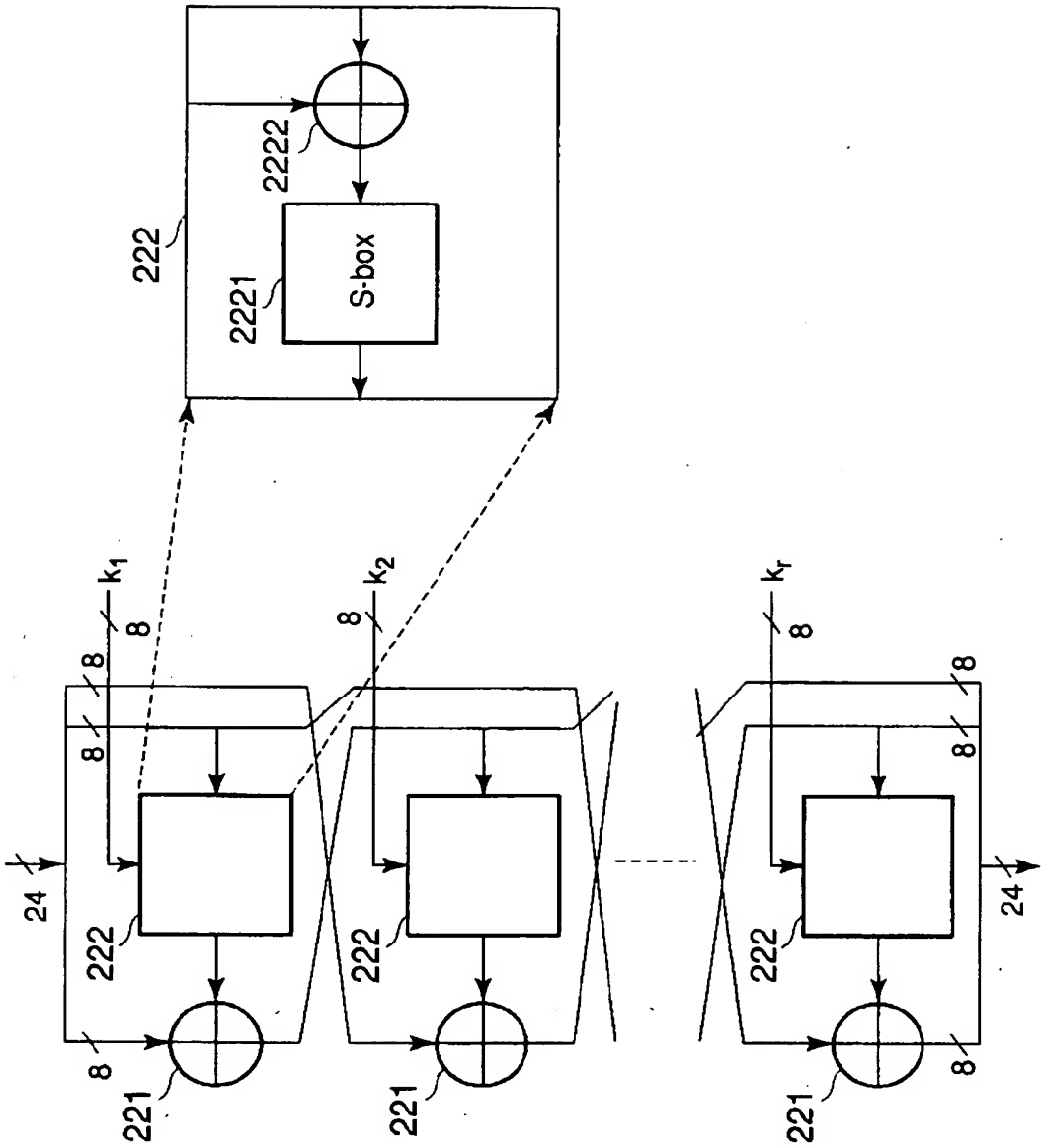
【図１６】



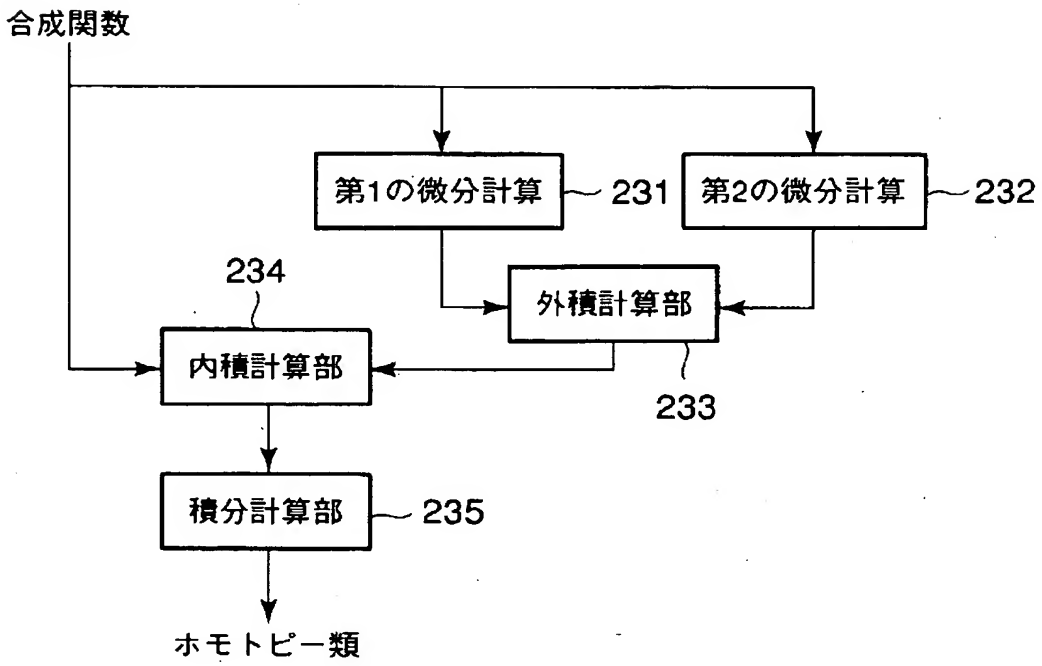
【図１７】


スタート
検出対象画像、鍵情報を入力する
S31
S32-1
S32-2
S32-3
g個のフレームから成るグループ2つの輝度値の差に埋め込まれた関数のX成分を読み取る
g個のフレームから成るグループ2つの輝度値の差に埋め込まれた関数のY成分を読み取る
g個のフレームから成るグループ2つの輝度値の差に埋め込まれた関数のZ成分を読み取る
鍵情報に従い、掻き混ぜ戻し関数を生成し、合成関数を計算する
S33
合成関数の属するホモトピー類を計算する
S34
ホモトピー類を透かし情報として出力する
S35
エンド

【図１８】



【図１９】


合成関数
第1の微分計算
231
第2の微分計算
232
234
外積計算部
内積計算部
233
積分計算部
235
ホモトピー類

【書類名】　　要約書

【要約】

【課題】　ＳｔｉｒＭａｒｋ攻撃やＤ－Ａ－Ｄ－変換などの局所的変形に対する耐性を持つとともに、電子透かしのアルゴリズムの全部又は一部が開示されたとしてもなお安全であるような電子透かしシステムを提供すること。

【解決手段】　コンテンツに透かし情報を埋め込む電子透かし埋込装置１は、埋め込むべき位相不変量を入力し、コンテンツの内容のうち透かし情報の埋め込みに供される部分を変更するごとによって、コンテンツに位相不変量を設定する。その際、埋め込みに先立って、鍵情報に基づく掻き混ぜを行っておく。透かし情報を埋め込まれたコンテンツは流通経路３を流通する。コンテンツから透かし情報を検出する電子透かし検出装置２は、コンテンツの内容のうち予め定められた部分に基づいて、コンテンツに設定された位相不変量を検出する。その際、検出に先立って、正しい鍵情報に基づく掻き混ぜ戻しを行っておく必要がある。

【選択図】　　図１

特願２００２－３８１３８０

出　願　人　履　歴　情　報

識別番号　　［０００００３０７８］

１．変更年月日　　２００１年　７月　２日
［変更理由］　　住所変更
住　所　　東京都港区芝浦一丁目１番１号
氏　名　　株式会社東芝

２．変更年月日　　２００３年　５月　９日
［変更理由］　　名称変更
住所変更
住　所　　東京都港区芝浦一丁目１番１号
氏　名　　株式会社東芝